

FactoryTalk® Security

System Configuration Guide



Table of contents

Preface	About this publication.....	11
	Required software	12
	Required hardware	12
	Additional resources	12
	Legal Notices	13
 Chapter 1		
FactoryTalk Security overview	Understanding automation security	17
	What problem does FactoryTalk Security solve?	18
	How does FactoryTalk Security protect the application layer?	18
	Where to start.....	20
 Chapter 2		
Plan your system	About the FactoryTalk system	21
	FactoryTalk Services Platform	21
	The FactoryTalk Directory	21
	Two directories on each computer.....	22
	Examples of FactoryTalk systems	22
	Example: Stand-alone system on a single computer.....	23
	Example: Distributed system on a network	24
 Chapter 3		
Install and activate FactoryTalk software	Before you begin.....	25
	What you need	26
	Follow these steps.....	27
	Install FactoryTalk-enabled software	27
	Step 1: Install Microsoft Internet Information Service	28
	Step 2: Install FactoryTalk Services Platform	28
	Step 3: Install FactoryTalk Activation Manager.....	29
	Step 4: Install RSSecurity Emulator software	30
	Step 5: Install and activate selected FactoryTalk View SE components	30
	Step 6: Install and activate RSLogix communications software	31
	Step 7: Install Microsoft SQL Server 2008 R2 Express	32
	Step 8: Install and activate RSLogix software.....	32
	Step 9: Install and activate FactoryTalk Batch Server and Client software.....	33
	Where to go from here	34

Create a user.....	71
Create a user group	74
Where to go from here	77

Chapter 6

Assigning permissions

Before you begin.....	79
What you need	79
Follow these steps	80
Allow and deny permissions	80
Understanding "inheritance"	81
Order of precedence	82
Categories of permissions for actions	83
Assigning permissions	83
Viewing permissions.....	85
Understanding effective permissions.....	85
Creating action groups	87
Create the action groups for our example scenario.....	87
Working with action groups.....	89
Where to go from here	91

Chapter 7

Setting up system-wide policies and product policies

Before you begin.....	94
What you need	94
Follow these steps	95
System-wide policies	95
Assigning system policies.....	96
Product policies.....	98
Product policies and inheritance	98
How are product policies and actions different?.....	99
Two different ways to configure feature security	99
Configure multiple products	99
Configuring a single product feature	100
Where to go from here	102

Chapter 8

Resource grouping

Before you begin.....	103
What you need	103
Follow these steps	104
Using resource groupings	104
Why is it called resource "grouping"?	104
Resource grouping and the Networks and Devices tree	104
How networks and devices inherit security permissions	105

Planning how to group resources	106
Creating exceptions for individual networks or devices.....	106
The same device cannot be a member of multiple resource groupings.....	106
Using the Resource Editor	107
Adding a logical name	108
Where to go from here	111

Chapter 9

RSLinx and FactoryTalk Security

Before you begin.....	113
What you need	113
Follow these steps	114
Install the Rockwell Software Security Emulator.....	114
Configuring RSLinx Classic to work with FactoryTalk Security.....	116
Configure security for RSLinx Classic	117
Assigning permissions	118
Considerations when using RSLinx Classic with FactoryTalk Security	122
What can I secure in RSLinx Classic?	123
Where to go from here	124

Chapter 10

Logix Designer application and FactoryTalk Security

Before you begin.....	125
What you need	125
Follow these steps	126
Enable security for Logix Designer application	126
Secure a Logix Designer Project File	129
Secure a Logix Designer project component	134
Configure a Secondary Security Authority	135
Apply security to a controller in FactoryTalk.....	136
Configure a permission set for use in Logix Designer	139
Give access to secured controller resources.....	141
Securing PLCs	147
Permission sets and logical names	147
Where to go from here	148

Chapter 11

FactoryTalk View SE and FactoryTalk Security

Before you begin.....	151
What you need	151
Follow these steps	152
Creating FactoryTalk Security accounts	152
Set up system and product policies	159

Product policies.....	160
System policies	161
Add FactoryTalk user accounts to FactoryTalk View	162
Where to go from here	174

Chapter 12

FactoryTalk View ME and FactoryTalk Security

Before you begin.....	176
What you need	176
Follow these steps	177
Creating FactoryTalk Security accounts.....	177
Add FactoryTalk user and group accounts	178
Add FactoryTalk user accounts to FactoryTalk View	184
Managing FactoryTalk Security for multiple applications	191
Back up the development application	192
Back up runtime application and FactoryTalk Local Directory ..	192
Restore the application to the runtime computer	194
Working with the 3.20 user account tab	196
Where to go from here	199

Chapter 13

FactoryTalk Batch and FactoryTalk Security

Before you begin.....	201
What you need	201
Follow these steps	203
Some important information on installing FactoryTalk Batch	203
Create FactoryTalk Batch users and groups	204
Configure FactoryTalk Batch Product Policies	209
Configuring security for the FactoryTalk Batch View windows	210
Configuring Security for FactoryTalk Batch Commands.....	213
Configure Equipment Editor and Recipe Editor security	217
Configure Access Mode security	218
Modifying the Equipment Editor configuration options.....	219
Where to go from here	221

Chapter 14

Deploying a FactoryTalk system

Assumptions.....	223
Setting up the development system computers	223
Step 1: On a Network Directory computer	223
Step 2: On the FactoryTalk View Site Edition Server computer	224
Step 3: On the FactoryTalk View Studio computer.....	224
Step 4: On the RSLinx Classic or RSLinx Enterprise computer	225
Step 5: On the Microsoft SQL Server computer.....	225
Step 6: On the FactoryTalk Transaction Manager computer.....	225

Step 7: On the FactoryTalk Batch Server computer	225
Step 8: On the FactoryTalk Batch client computers	225
On the runtime system computers.....	226
Step 1: On a Network Directory computer	226
Step 2: On the FactoryTalk View Site Edition Server computer	227
Step 3: On the FactoryTalk View Site Edition Client computers.....	228
Step 4: On the RSLinx Classic computer	228
Step 5: On the RSLinx Enterprise server computer.....	228
Step 6: On the Microsoft SQL Server computer.....	229
Step 7: On the FactoryTalk Transaction Manager computer.....	230
Step 8: On the FactoryTalk Batch Server computer	231
Step 9: On the FactoryTalk Batch client computers	231
Backing up an entire FactoryTalk Directory	231
Required security permissions	231
To back up a FactoryTalk Directory:.....	231
Restore a FactoryTalk Directory.....	233
Required security permissions	233
To restore a FactoryTalk Directory:	233
After restoring a FactoryTalk Directory	236
After restoring an entire FactoryTalk Directory	236
After restoring the FactoryTalk Directory contents.....	238
After restoring the FactoryTalk Directory security authority identifier.....	239

Appendix A

Upgrade FactoryTalk Services Platform

Before you begin.....	241
When upgrading FactoryTalk platform software.....	241
When upgrading computers in a distributed system	242
Identifying the installed version of the FactoryTalk platform	244
What you need	244
Installing FactoryTalk Services Platform	244
Import Status Text File	248
Organizer Import Result	249
Resource Editor.....	250

Appendix B

Install FactoryTalk Web Services

Install Microsoft Internet Information Services.....	251
To install IIS for Windows Server 2008 or Server 2012	252
To install IIS for Windows 7, Windows 8, or Windows 8.1	253
Install FactoryTalk Web Services.....	256
To check that the FactoryTalk Security Web Service is working	257
If the Web Service is not working	258

Appendix C

What's a FactoryTalk Directory

Creating your own FactoryTalk system.....	261
Understanding FactoryTalk Directories.....	262
Choosing a directory for FactoryTalk Security	263

Appendix D

FactoryTalk Directory Configuration Wizard Index

When to run the FactoryTalk Directory Configuration Wizard.....	265
Running the FactoryTalk Directory Configuration Wizard.....	266

About this publication

This guide is intended for use by those who are new to FactoryTalk Security. Most of the chapters in this guide are modular — you can refer to only those sections that provide the information you need without having to read the entire document. However, it is recommended that you read at least Chapters 1, 2 and 3, as they will give you an overall understanding of FactoryTalk Security and how it works.

Tip: If you are not new to RSAssetSecurity or RSSecurity Server, this guide can be used to learn the new features introduced in version 9.0 (CPR 9). Refer to Appendix A for information on migrating an RSSecurity Server database or upgrading from RSAssetSecurity (CPR 7) to FactoryTalk Security (CPR 9).

The information provided in this guide is divided into the following chapters:

- **Chapter 1** gives you a brief introduction to automation security and how FactoryTalk Security can be used to help tighten your application security.
- **Chapter 2** is an overview of how FactoryTalk Security integrates with other FactoryTalk-enabled products and the FactoryTalk Services Platform. You are also given an overview of planning a FactoryTalk system.
- **Chapters 3 and 4** walk you through installing and configuring FactoryTalk Security, which is installed with the FactoryTalk Services Platform.
- **Chapters 5, 6, and 7** show you how to fine-tune your FactoryTalk Security installation by creating user and user group accounts, assigning permissions to those users and groups, and setting up system-wide security policies.
- **Chapter 8** delves into the more advanced features of FactoryTalk Security and how you can tighten security even more.
- **Chapters 9 through 13** walk you through configuring FactoryTalk Security for use with other FactoryTalk-enabled products, like FactoryTalk View SE and FactoryTalk Batch. These chapters also show you how to configure FactoryTalk Security to work with RSLinx Classic and Studio 5000™ Logix Designer application, which are not currently FactoryTalk-enabled.
- **Chapter 14** discusses deploying a FactoryTalk system from a test environment to a production environment once you have everything configured and tested to your satisfaction.

Throughout this guide, you will be given references to guides and online help files that have more detailed information on the products and services discussed in this guide. There are also tips, important notes, best practices, and the occasional caution included in the document to help you become more adept at using the product.

Required software

FactoryTalk Services Platform and Windows operating system software are required for configuring and operating FactoryTalk Security. FactoryTalk Security is one of many shared services that installs as part of the FactoryTalk Services Platform.

Important: This guide briefly discusses the installation of many products and does not go into detail unless something other than the default installation options is required. For more detailed instructions, refer to each product's installation documentation.

FactoryTalk Services Platform installs as part of each FactoryTalk product's installation process. The options available to you depend on which product you are installing. Some products may prompt you to make choices as part of the installation process, while others may install the FactoryTalk Services Platform behind the scenes.

- FactoryTalk Services Platform, v. 2.10 or later – includes FactoryTalk Administration Console, FactoryTalk Directory, FactoryTalk Diagnostics, and FactoryTalk Security services.
- One of the following Microsoft Windows operating systems:
 - Windows 8.x
 - Windows 7 Professional with Service Pack 1 and Windows 7 Home Premium with Service Pack 1
 - Windows Server 2012 Standard
 - Windows Server 2012 Datacenter
 - Windows Server 2012 R2
 - Windows Server 2012 R2 Datacenter
 - Windows Server 2008 Standard with Service Pack 2
 - Windows Server 2008 R2 Standard with Service Pack 1
- FactoryTalk-enabled software that supports FactoryTalk Security.

Required hardware

Hardware requirements depend upon the type of system you intend to develop and the software products you plan to install. For guidelines, see each product's installation instructions.

Additional resources

For more information on the products and components discussed in this guide, the following manuals and Help files are available:

- FactoryTalk Help – From the Windows **Start** menu, select **All Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Help**
- FactoryTalk View Installation Guide or FactoryTalk View Help – In FactoryTalk View Studio, select **Help > Online Books > Installation Guide** or **Help > Contents**

- RSLinx Enterprise Help – From the Windows **Start** menu, select **Start > All Programs > Rockwell Software > RSLinx > RSLinx Classic Online Reference**. On the **Contents** tab, expand the **How To** and **Secure RSLinx Classic with FactoryTalk Security** books, and then select **What can I secure in RSLinx Classic?**
- RSLinx Classic Help – From the Windows **Start** menu, select **Start > All Programs > Rockwell Software > RSLinx > RSLinx Classic Online Reference**. On the **Contents** tab, expand the **How To** and **Secure RSLinx Classic with FactoryTalk Security** books, and then select **What can I secure in RSLinx Classic?**
- Logix Designer application Help – In Logix Designer application, select **Help > Contents**
- FactoryTalk Batch Administrator's Guide – From the Windows **Start** menu, select **Start > All Programs > Rockwell Software > FactoryTalk Batch Suite > FactoryTalk Batch > Online Books > FactoryTalk Batch > Batch Administrator's Guide**
- FactoryTalk Transaction Manager Help
- FactoryTalk AssetCentre Help

Legal Notices

Copyright notice

© 2015 Rockwell Automation, Inc. All rights reserved. Printed in USA.

This document and any accompanying Rockwell Software products are copyrighted by Rockwell Automation, Inc. Any reproduction and/or distribution without prior written consent from Rockwell Automation, Inc. is strictly prohibited. Please refer to the license agreement for details.

End User License Agreement (EULA)

You can view the Rockwell Automation End-User License Agreement ("EULA") by opening the License.rtf file located in your product's install folder on your hard drive.

Other Licenses

Distributed under the Boost Software License, version 1.0. See accompanying file LICENSE_1_0.txt at http://www.boost.org/LICENSE_1_0.txt
http://www.boost.org/LICENSE_1_0.txt.

Trademark Notices

Allen-Bradley, ControlLogix, CompactLogix, Connected Components Workbench, FactoryTalk, GuardLogix, Micro800, MicroLogix, MobileView, MobileView Guard, PanelBuilder, PanelView, PhaseManager, PlantLink, PlantPAX, PLC-2, PLC-3, PLC-5, PowerMonitor, Rockwell Automation,

Rockwell Software, SLC, SoftLogix, Studio 5000, and XM are trademarks of Rockwell Automation, Inc.

Any Rockwell Automation software or hardware not mentioned here is also a trademark, registered or otherwise, of Rockwell Automation, Inc.

Other Trademarks

Contains BIGDIGITS multiple-precision arithmetic code originally written by David Ireland, Copyright © 2001-2005 by D.I. Management Services Pty Limited www.di-mgt.com.au, and is used with permission.

Portions Copyright© 1999-2006 The Botan Project.

Portions Copyright © 2001-2002 Expat Maintainers, Copyright © 1998-2000 Thai Open Source Software Center Ltd and Clark Cooper.

Portions Copyright © 1999-2000 Boris Fomitchev, Copyright © 1997 Moscow Center for SPARC Technology, Copyright © 1996-1997 Silicon Graphics Computer Systems, Inc. Copyright © 1994 Hewlett-Packard Company.

All other trademarks are the property of their respective holders and are hereby acknowledged.

Warranty

This product is warranted in accordance with the product license. The product's performance may be affected by system configuration, the application being performed, operator control, maintenance, and other related factors. Rockwell Automation is not responsible for these intervening factors. The instructions in this document do not cover all the details or variations in the equipment, procedure, or process described, nor do they provide directions for meeting every possible contingency during installation, operation, or maintenance. This product's implementation may vary among users.

This document is current as of the time of release of the product; however, the accompanying software may have changed since the release. Rockwell Automation, Inc. reserves the right to change any information contained in this document or the software at any time without prior notice. It is your responsibility to obtain the most current information available from Rockwell when installing or using this product.

Environmental compliance

Rockwell Automation maintains current product environmental information on its website at <http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page>

<http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page>

Contact Rockwell

Customer Support Telephone — 1.440.646.3434

Online Support — <http://www.rockwellautomation.com/support/>
<http://www.rockwellautomation.com/support/>

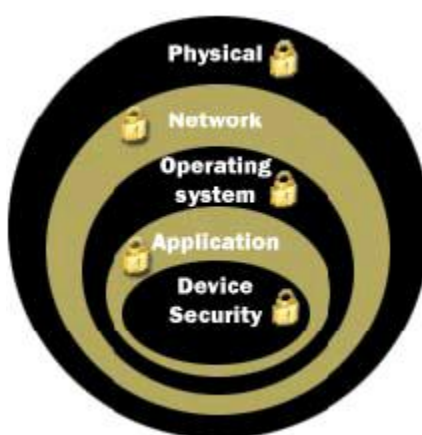
FactoryTalk Security overview

This chapter gives you a brief introduction to automation security, introduces new terms and concepts, and discusses how FactoryTalk Security can be used to help tighten application security.

Understanding automation security

Securing an integrated, distributed automation system from both internal and external threats requires working across multiple disciplines to develop a multi-layered solution. Security experts call this type of solution a "defense-in-depth" architecture. In simple terms, this means applying different layers or defenses at different levels across an automation system to address different threats. For example, layers of security might include specific solutions for defending an automation system from a facility's outside walls all the way down through the system to hardware devices on the plant floor. Typical security layers include:

- Physical security
- Network security
- Operating system security
- Application security
- Device security



Before applying security solutions, however, we must understand the problems that need to be solved, and then calculate the return on investment for each security solution.

The first step for any organization is to determine the value of all business assets, including equipment, people, products, production, reputation,

intellectual property, and so on, and the potential costs associated with the loss of any of these assets. It is also important to understand the threats to these assets that could disrupt normal business activities. These threats could be internal or external, and could be either malicious or accidental.

The next step is to calculate risks and design a plan to defend against the most expensive threats with the highest probability of occurring. Design a plan that mitigates only those threats that exceed your organization's risk threshold. Implementing security solutions is a lot like shopping for insurance – purchase only enough insurance to reduce the perceived risk to an acceptable level. Just as you would not spend more on insurance than the cost of the asset to be protected, the same is true for evaluating the cost-benefit ratio for implementing security solutions.

What problem does FactoryTalk Security solve?

In terms of the layered security model above, FactoryTalk Security is designed to provide a layer of **application security**. Its purpose is to protect against internal threats that are either malicious or accidental by **limiting access** to only those individuals who legitimately need access to specific automation assets. FactoryTalk Security accomplishes this goal by allowing security administrators to define the answer to this question:

"Who can carry out what actions upon which secured resources from where?"

- **Who** can use Rockwell Automation **software products**
- to perform **what** specific **actions**
- on **which** Rockwell Automation **hardware devices** and other securable resources
- from **where** - that is, from specific computers or workstations

How does FactoryTalk Security protect the application layer?

When someone attempts to use a FactoryTalk-enabled software product to access a Rockwell Automation hardware device or other securable resource, FactoryTalk Security **authenticates** the person's identity and **authorizes** that person to access that resource and perform only allowed actions.

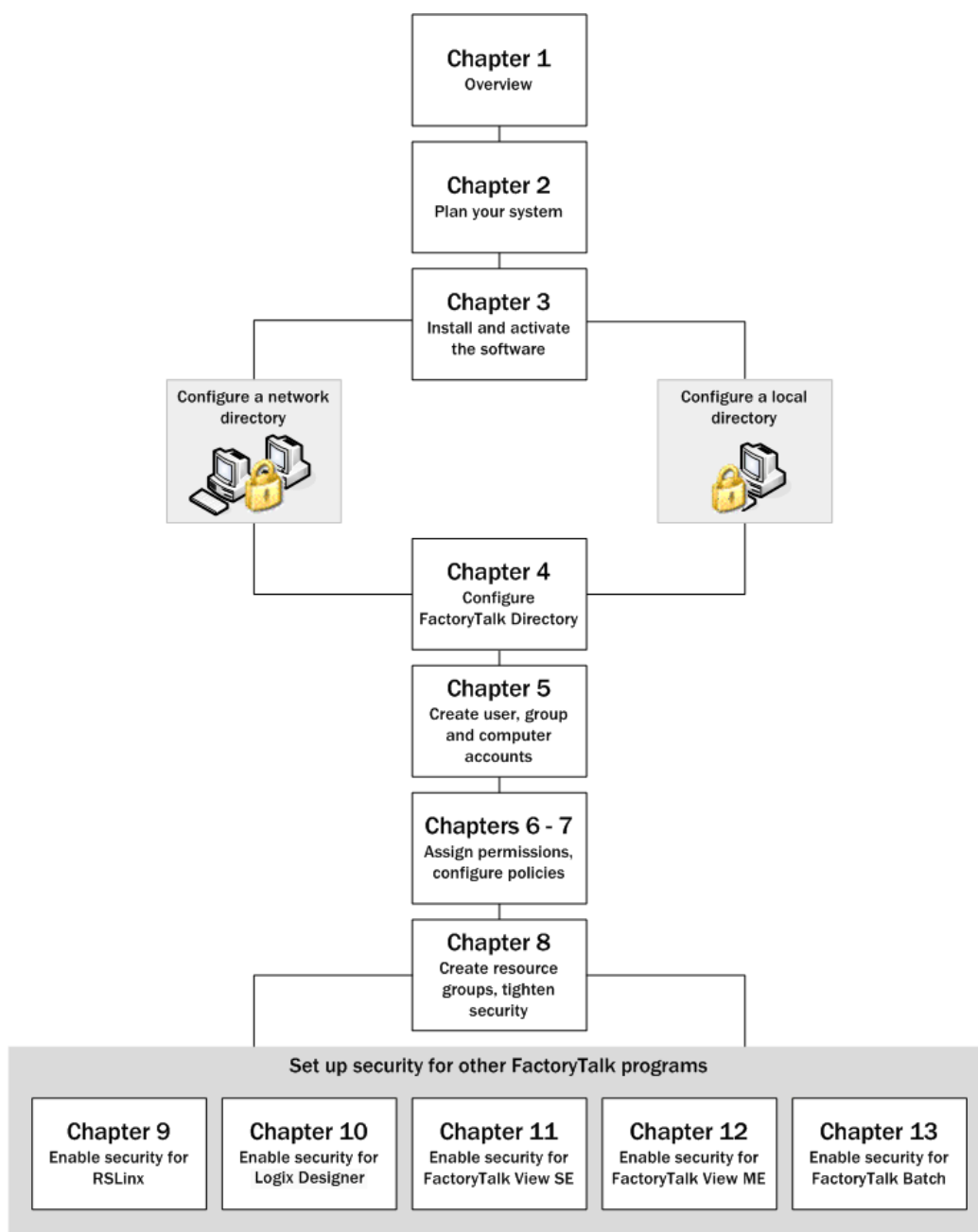
- **Authentication.** Verifies a user's identity and verifies that a request actually originated with that user.
- **Authorization.** Verifies a user's request to use a software product or to access a hardware device or secured resource against a set of previously defined access permissions.

FactoryTalk Security allows centralized administration of user accounts and access permissions. Security information, including user authentication and authorization, can be shared across all software products and hardware

devices on a particular computer, throughout a plant, or across an entire enterprise.

Tip: For comprehensive information about FactoryTalk Security, see FactoryTalk Security Help, available from Windows **Start > All Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Help**.

Where to start



Plan your system

About the FactoryTalk system

FactoryTalk Security services are fully integrated into the FactoryTalk Directory and are always present wherever the FactoryTalk Services Platform software is installed. Use FactoryTalk Administration Console or FactoryTalk View Studio to administer centralized security services.

A FactoryTalk system is made up of FactoryTalk-enabled software products, services, and hardware devices all participating together and sharing the same FactoryTalk Services Platform and FactoryTalk Directory.

FactoryTalk Services Platform is an underlying architecture and set of services that software products can build upon. Products in the FactoryTalk suite include FactoryTalk View, RSLinx, RSLogix, FactoryTalk Batch, FactoryTalk AssetCentre, and FactoryTalk Transaction Manager, among others.

FactoryTalk Services Platform

- Provides common services (such as diagnostic messages, health monitoring services, and access to real-time data) and shares plant resources (such as tags and graphic displays) across an automation system.
- Supports centralized security services.
- Supports centralized alarm and event services.

The FactoryTalk Directory

The FactoryTalk Directory references tags, data servers, security settings, and other project information from multiple data sources, and then makes this information available through a lookup service to all software products participating in an application.

An **application** organizes project information, including elements such as data servers, HMI servers, and alarm and event servers, and makes it available to all participating software products and computers. A FactoryTalk Directory can contain multiple applications.

- **Network applications** are held in a *FactoryTalk Network Directory*. Project information and software products can be located on multiple

computers distributed across a network. All of the computers participating in a particular Network application share a common Network Directory Server located on a network computer.

- **Local applications** are held in a *FactoryTalk Local Directory*. Project information is located on a stand-alone computer and is available only to software products installed on that same local computer. Local applications cannot be accessed remotely and cannot share project information with a Network application.

Two directories on each computer

The FactoryTalk Services Platform installs and configures both a **Local Directory** and a **Network Directory** on each computer. All of the project information and security settings remain completely separate and cannot be shared between the two directories, including:

- user accounts, passwords, security permissions
- system-wide policy settings, including security and audit policies
- project information, such as applications, area, and their contents

Which directory you need depends upon which software products you plan to use and whether you plan to work in a stand-alone or a networked environment. Consult your product documentation for details.

A FactoryTalk system is comprised of software products, services, and hardware devices participating together and sharing the same FactoryTalk Directory.

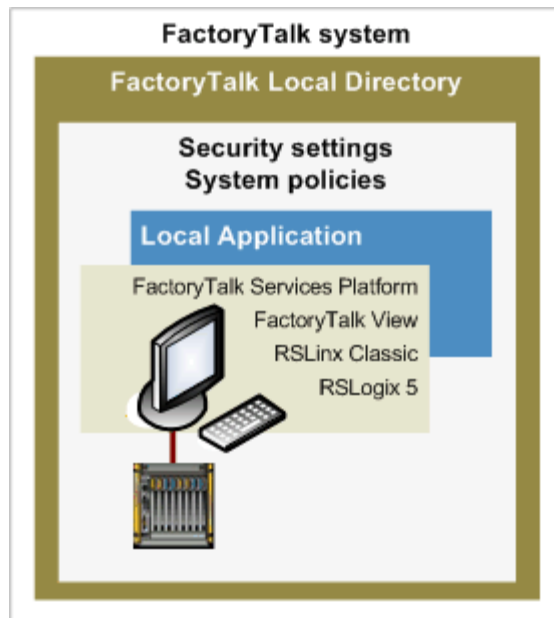
If you plan to run a FactoryTalk system on a stand-alone computer, install and activate all FactoryTalk products and services on that same computer, and then create Local applications using the FactoryTalk Local Directory.

If you plan to run a FactoryTalk system on multiple computers distributed across a network, install and activate FactoryTalk products services across those computers, and then create Network applications using the FactoryTalk Network Directory.

Examples of FactoryTalk systems

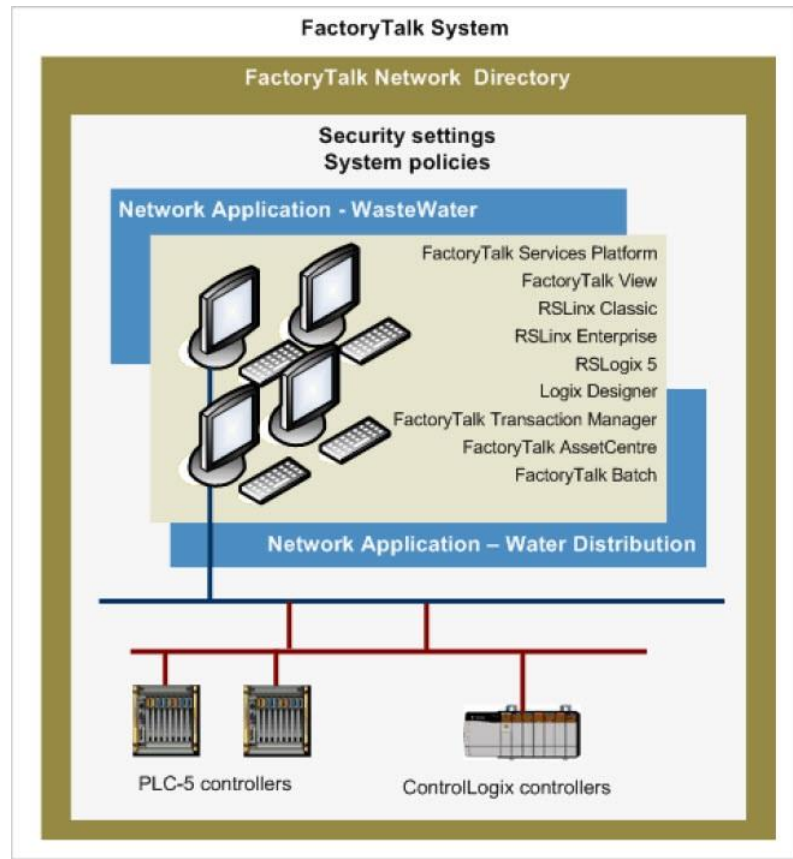
Example: Stand-alone system on a single computer

For example, a FactoryTalk system may be as simple as FactoryTalk Services Platform, FactoryTalk View, RSLinx Classic, and RSLogix 5 all installed on the same computer, communicating with a single programmable logic controller, and all participating in the same Local application held in a Local Directory.



Example: Distributed system on a network

A FactoryTalk system may be complex, with software products and hardware devices participating in multiple Network applications distributed across a network, all sharing the same Network Directory.



In the Network Directory example above, the FactoryTalk Network Directory hosts two Network applications: one named Waste Water and the other named Water Distribution. All of the areas, data servers, HMI servers, device servers, and alarm and event servers organized within each application are specific to that application. None of the application-specific information is shared with any other application in the directory. However, security settings, system policies, product policies, user accounts, and so on, apply to all applications that share the same FactoryTalk Directory.

Install and activate FactoryTalk software

This chapter outlines the steps for getting FactoryTalk Security up and running.

FactoryTalk Security software does not install separately — it installs as an integrated part of the FactoryTalk Services Platform.

You can install FactoryTalk Services Platform from either:

- a FactoryTalk product installation disc, such as FactoryTalk View (FactoryTalk Services Platform software is included on the installation disc of every product that requires it); or,
- the Rockwell Automation Knowledgebase website <http://www.rockwellautomation.com/knowledgebase/>. On the Knowledgebase page, click **Find Technical Support Answers**. On the Answers page, in the Search box, type **FTSP Downloads**, and click **Search**. From the search results, select the technical note that includes FactoryTalk Services Platform downloads.

The installation disk you will use depends upon which FactoryTalk-enabled software products you have purchased. For details, refer to each product's installation instructions.

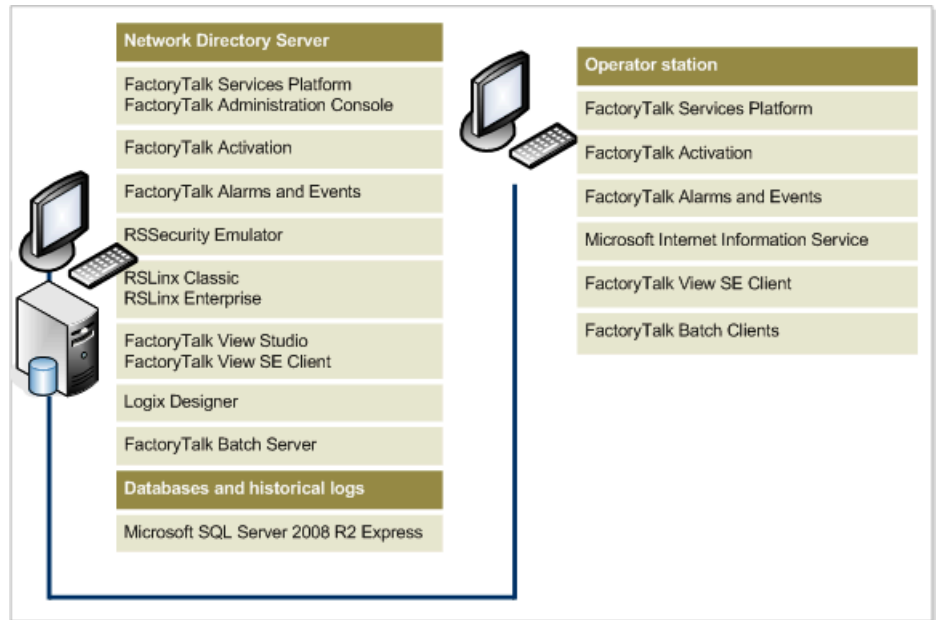
Important:	This guide assumes that you are installing FactoryTalk Services Platform for the first time on each computer in your network, and that you are not upgrading from earlier versions of any of the software. If you are upgrading from earlier versions, like RSAssetSecurity, see Upgrade FactoryTalk Services Platform on page 241 .
-------------------	--

Before you begin

This guide provides examples for working with a FactoryTalk Network Directory on a distributed system. If you plan to work with a FactoryTalk Local Directory, install all FactoryTalk software products on the same computer.

Before installing any FactoryTalk software, first determine which computers and operating systems you plan to use, and where you plan to install which software. For help developing your installation plan, consult this guide and individual product installation guides.

The following diagram shows an example of the network layout for a group of computers and software products participating in Network Directory distributed across multiple computers. This is the system we will be setting up throughout this guide.



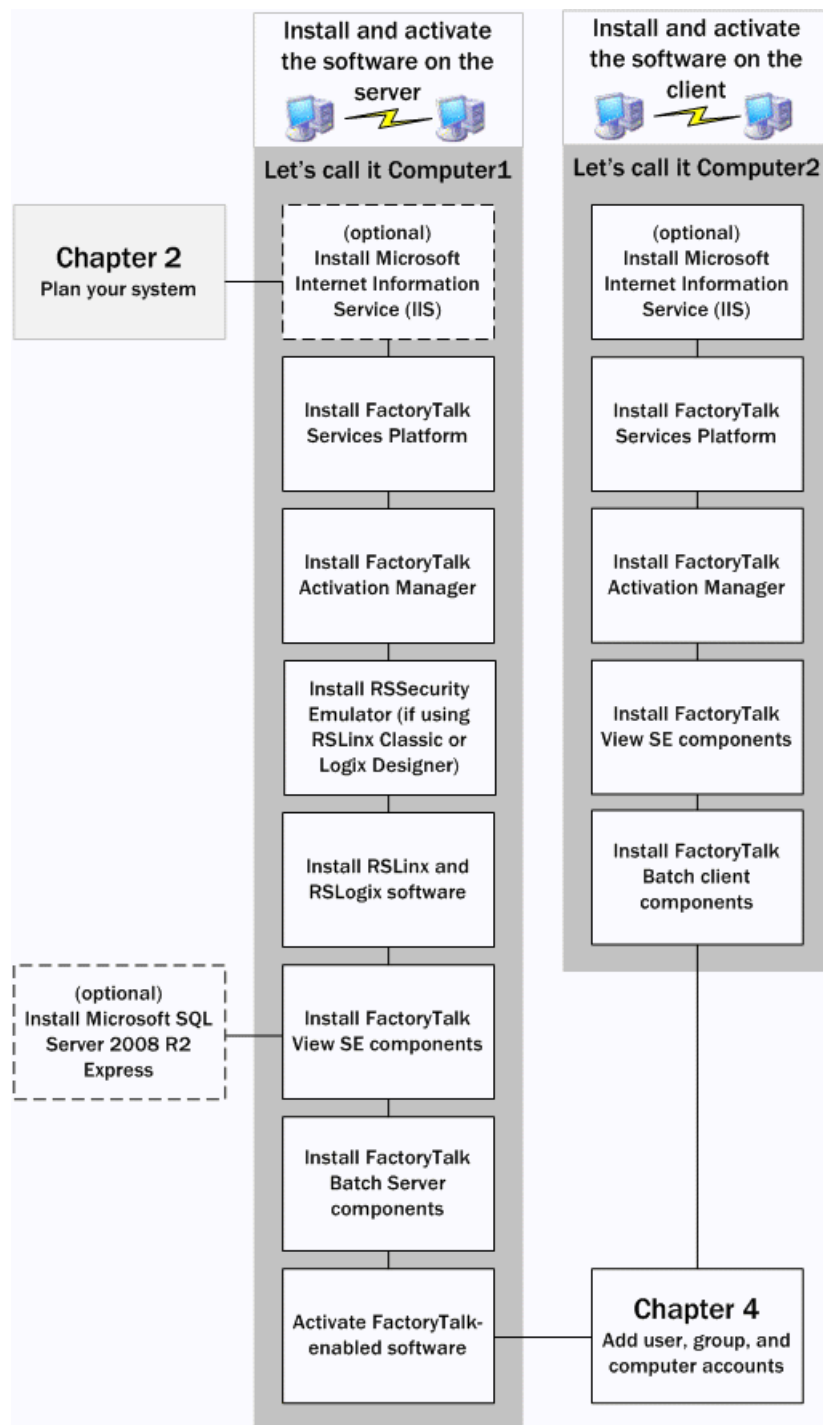
For more details and examples of the types of FactoryTalk systems possible, refer to the FactoryTalk Help.

What you need

- At least two personal computers on a network (see each product's installation instructions for hardware and operating system requirements)
- FactoryTalk View (CPR 9 or later) installation disc (or other FactoryTalk-enabled product installation disc). Using the newest available version is recommended.
- Studio 5000 installation disc (optional)
- Access to the Internet (to activate the software)
- Installation guides for each of the Rockwell Automation software products you plan to install

Important: The information contained in this guide is intended to give you a high-level look at FactoryTalk Security and how it is used with FactoryTalk-enabled products. This guide walks you through installing and configuring security on two computers (where appropriate); one will be configured as a server, the other as a client.

Follow these steps



Install FactoryTalk-enabled software

The steps below outline the high-level procedures for installing the FactoryTalk Services Platform and FactoryTalk-enabled software.

Important: This guide briefly discusses the installation of many products and does not go into detail unless something other than default installation options is required. For more detailed instructions, refer to each product's installation documentation.

Step 1: Install Microsoft Internet Information Service

To create and run FactoryTalk View SE network distributed applications, and allow other computers to view and modify components such as graphic displays, you must install Microsoft Internet Information Service (IIS) on every computer where you plan to install FactoryTalk View SE Server software. It is not necessary to install IIS on client computers. For step-by-step instructions, see the *FactoryTalk View Site Edition Installation Guide*.

You must also install Microsoft IIS server if you want to use the FactoryTalk Web Services feature. To read about the feature, see [Install FactoryTalk Web Services](#) on [page 256](#).

Step 2: Install FactoryTalk Services Platform

To install FactoryTalk Services Platform, you must log on to Windows with a user account that is a member of the Windows Administrators group on the local computer.

Install FactoryTalk Services Platform on every computer where you plan to develop or run Network or Local applications.

Example: For the examples used in this guide, you will be configuring a Network Directory on one computer, which will act as the server. This computer will be referred to as **Computer1**. A second computer will be configured as a client computer and will be referred to as **Computer2**.

Platform components and services currently include:

- FactoryTalk Directory
- FactoryTalk Security
- FactoryTalk Diagnostics
- FactoryTalk Live Data
- FactoryTalk Administration Console – a stand-alone tool for configuring, managing, and securing applications.

All of these components and services install together as a platform, integrated into the software install process for each FactoryTalk-enabled product. For step-by-step instructions, see each product's installation instructions.

On Computer1: Install FactoryTalk Services Platform. This is the FactoryTalk Directory server computer.

On Computer2: Install FactoryTalk Services Platform. After FactoryTalk Services Platform is installed, run the **FactoryTalk Directory Server Location Utility** and point to **Computer1** as the Network Directory server.

Step 3: Install FactoryTalk Activation Manager

FactoryTalk Activation provides a secure, software-based system for activating Rockwell Software products and managing software activation files. With FactoryTalk Security, you can develop and manage a centralized security system for multiple applications distributed across an entire automation network.

FactoryTalk Activation Manager makes FactoryTalk product activations available to the FactoryTalk Network Directory Server computer.

Install FactoryTalk Activation Manager on both **Computer1** and **Computer2**. For detailed information on installing FactoryTalk Activation, refer to the printed insert, *Activate Rockwell Software Products* (shipped with your product package) or FactoryTalk Activation Help.

The activation server can be the same as the Network Directory Server. It can also be a different computer that is not restarted frequently, for example, another server computer.

You can add the location of a computer that will provide activations and display existing activations that have already downloaded to an activation server.

Get FactoryTalk product activations

Do one of the following:

- **If the computer has Internet access**, run FactoryTalk Activation Manager. In the **Manage Activations** tab, click **Get New Activations** and select the activation method you want to use. Follow the instructions to get your activations.
- **If the computer does NOT have Internet access**, refer to the FactoryTalk Activation Manager Help for instructions.

Click the **Help** button on the **FactoryTalk Activation Manager** dialog box for further instructions on getting activations.

Some FactoryTalk-enabled software products prompt for activation at the end of the installation process. If you have already got activations for the products you are installing, you do not need to run FactoryTalk Activation Manager.

Tip: To save time, get activations for all of the FactoryTalk-enabled products you have installed, or are going to install. Do not forget to activate the software installed on the Client computer(s).

Step 4: Install RSSecurity Emulator software

Optional. This step applies if you are going to be using RSLinx Classic or Logix Designer application with FactoryTalk Security.

For products that do not currently support FactoryTalk Security, the RSSecurity Emulator allows you to configure users, groups, security permissions, and so on, in one place, and then share those settings among the client software products, such as RSLinx Classic and Logix Designer application.

Tip: If you are currently using RSSecurity Server and are upgrading to FactoryTalk Security, refer to [Installing FactoryTalk Services Platform](#) on [page 244](#) and to *Migrating RSSecurity to FactoryTalk Security* in the FactoryTalk Security online Help.

To use the RSSecurity Emulator, install it on every computer where RSLinx Classic and Logix Designer application are going to be installed, which will only be **Computer1** for the examples used in this guide. Once installed, you do not have to do anything to make the RSSecurity Emulator run.

For step-by-step instructions, see [Install the Rockwell Software Security Emulator](#) on [page 114](#).

Example: For the examples used in this guide, you will be configuring a Network Directory. Select **Network Directory** when prompted.

Step 5: Install and activate selected FactoryTalk View SE components

FactoryTalk View SE consists of several software components, for example, FactoryTalk View SE Client, FactoryTalk View SE Server, and FactoryTalk View Studio.

When you opt to install selected components, you can choose which individual components, or combination of components, you want to install on the computer.

Installing FactoryTalk View software also installs FactoryTalk Activation and FactoryTalk Alarms and Events software. FactoryTalk View SE requires a Windows network and relies on a number of Windows elements, including Internet Information Services (IIS).

For step-by-step instructions, see the FactoryTalk View Site Edition Installation Guide.

On Computer1: Install the FactoryTalk View SE Server components on the same computer as the FactoryTalk Network Directory server. Select **Network Directory** when prompted to choose a FactoryTalk Directory during installation.

Tip: Since the FactoryTalk View installation prompts you to specify the Network Directory location, install the software on the Network Directory Server computer first, and then install the View client components on other computers and point them to the Network Directory Server computer.

On Computer2: Install the FactoryTalk View SE Client components (like FactoryTalk View Studio) on the same client computer where FactoryTalk Activation Manager is installed. Select **Network Directory** when prompted to choose a FactoryTalk Directory during installation.

Step 6: Install and activate RSLinx communications software

RSLinx Classic and RSLinx Enterprise are families of software products that link Allen-Bradley networks and devices to Microsoft Windows products such as the FactoryTalk View family of visualization software and the RSLogix family of device programming software.

Two versions of RSLinx are commonly used in FactoryTalk systems:

- **RSLinx Classic** – an OPC-DA 2.0 data server.
- **RSLinx Enterprise** – a FactoryTalk Live Data server and device-based alarm and event server. Installing RSLinx Enterprise also installs FactoryTalk Alarms and Events software.

To allow RSLinx Classic to work with FactoryTalk Security, first install RSSECURITY Emulator software on every computer where you also plan to install RSLinx Classic. See [Install the Rockwell Software Security Emulator](#) on [page 114](#). See also the RSLinx Installation Guides.

Example: For the examples used in this guide, install RSLinx on **Computer1**.

Activate RSLinx Enterprise

RSLinx Enterprise (CPR 9 or later) supports the following activation tools:

- **FactoryTalk Activation™:** If you are a new user, you will need to activate your software using FactoryTalk Activation.
- **EvRSI activation:** If you are a current user upgrading to CPR 9 or later, your activation is already installed and will be used automatically.

Step 7: Install Microsoft SQL Server 2008 R2 Express

If you plan to use FactoryTalk Alarms and Events, install Microsoft SQL Server 2008 R2 Express, if no Microsoft SQL Server database is installed on a computer on the network. You need a compatible version of Microsoft SQL Server installed to log historical alarms and events to a database.

Print and refer to the detailed installation instructions included in the FactoryTalk Alarms and Events System Configuration Guide. This guide is available in the Docs folder on the FactoryTalk View installation disc. It is also available from the **Help > Online Books** menu in FactoryTalk View Studio.

Tip: If you plan on storing FactoryTalk Batch recipes in a SQL database, you must have a compatible version of Microsoft SQL Server installed before installing FactoryTalk Batch.

Step 8: Install and activate RSLogix software

The RSLogix family of software products provides programming software for Allen-Bradley control devices, including the Logix5000 family of controllers, PLC-5s, and SLC 500s.

To allow the Logix Designer application to work with FactoryTalk Security, first install RSSecurity Emulator software on every computer where you also plan to install RSLogix software. See [Install the Rockwell Software Security Emulator](#) on [page 114](#).

Example: For the examples used in this guide, install Logix Designer application on **Computer1**.

For information about enabling security for Logix Designer application, see [Logix Designer application and FactoryTalk Security](#) on [page 125](#).

Tip: RSSECURITY Emulator is not required for RSLogix 5 and RSLogix 500 software. For migrating from RSSECURITY Server, see *Migrating RSSECURITY to FactoryTalk Security* in the FactoryTalk Security Help.

- To program controllers, RSLinx Classic must be installed on the same computer as RSLogix.
- RSLinx Classic Lite, which comes with RSLogix, can be used only to program controllers; it cannot be used as a data server. To provide tag information to FactoryTalk clients, install RSLinx Classic, RSLinx Classic Gateway, or RSLinx Enterprise on the same computer as RSLogix.

Step 9: Install and activate FactoryTalk Batch Server and Client software

You **must** create a Windows user account for the FactoryTalk Batch Server **prior** to installing the FactoryTalk Batch software (for the examples used in this guide, we will use **batchsvr**). When you install FactoryTalk Batch components you are prompted to enter this user account to allow the installation program to configure your FactoryTalk Batch system.

On Computer1 and Computer2: Create a FactoryTalk Batch Server user account

When creating the Server user account, the following configuration requirements must be met.

- **The password should be configured to never expire**
If the password ever expires, the Batch Server service will fail to log on.
- **The Server user account should never be disabled or deleted**
If this account is ever disabled/deleted, the Batch Server service will fail to log on.
- **The domain user account should have a unique name**
If the Server user account is a domain account, remove any local user accounts with the same name.
- **The Server user account/user group must exist on all workgroup computers**

If you are using a local account and expect that account to have access to resources on other computers in a workgroup environment, you must create accounts with the same name and password on each computer in the workgroup.

Example: For the examples given in this guide, we will use **batchsvr** for the Batch Server user account. For more detailed instructions on creating user accounts, refer to the *FactoryTalk Batch Administrator's Guide*.

Install Microsoft SQL Server

- If you plan to store FactoryTalk Batch recipes in a SQL database, first install a compatible version of Microsoft SQL Server.

On Computer1: Install the FactoryTalk Batch Server components

Install the Server components on the same computer as the FactoryTalk Network Directory server. Select **Network Directory** when prompted to choose a FactoryTalk Directory during installation.

On Computer2: Install the FactoryTalk Batch Server components

Install the FactoryTalk Batch Server components (like Recipe Editor and Equipment Editor) on the same client computer where the FactoryTalk Activation Manager is installed. Select **Network Directory** when prompted to choose a FactoryTalk Directory during installation. When prompted for the Batch Server name, use the name of the computer where the Batch Server was installed.

For step-by-step instruction on installing FactoryTalk Batch components, see the *FactoryTalk Batch Installation Guide*.

Where to go from here

Do one of the following:

- Go to [Getting started with FactoryTalk Security](#) on [page 37](#) to learn about the FactoryTalk Administration Console
- Go to [Creating user accounts](#) on [page 67](#) to learn about creating user, group, and computer accounts.
- Go to [Assigning permissions](#) on [page 79](#) to learn about assigning permissions to the users, groups, and computers added in this chapter.
- Go to [Setting up system-wide policies and product policies](#) on [page 93](#) to learn about setting system-wide and policy-wide security policies.
- Go to [Resource grouping](#) on [page 103](#) to learn about FactoryTalk Security advanced features, such as resource grouping and tightening security.
- Go to [RSLinx and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLinx software.

- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure projects and devices like Logix5000, PLC, and SLC controllers.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components
- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.

Getting started with FactoryTalk Security

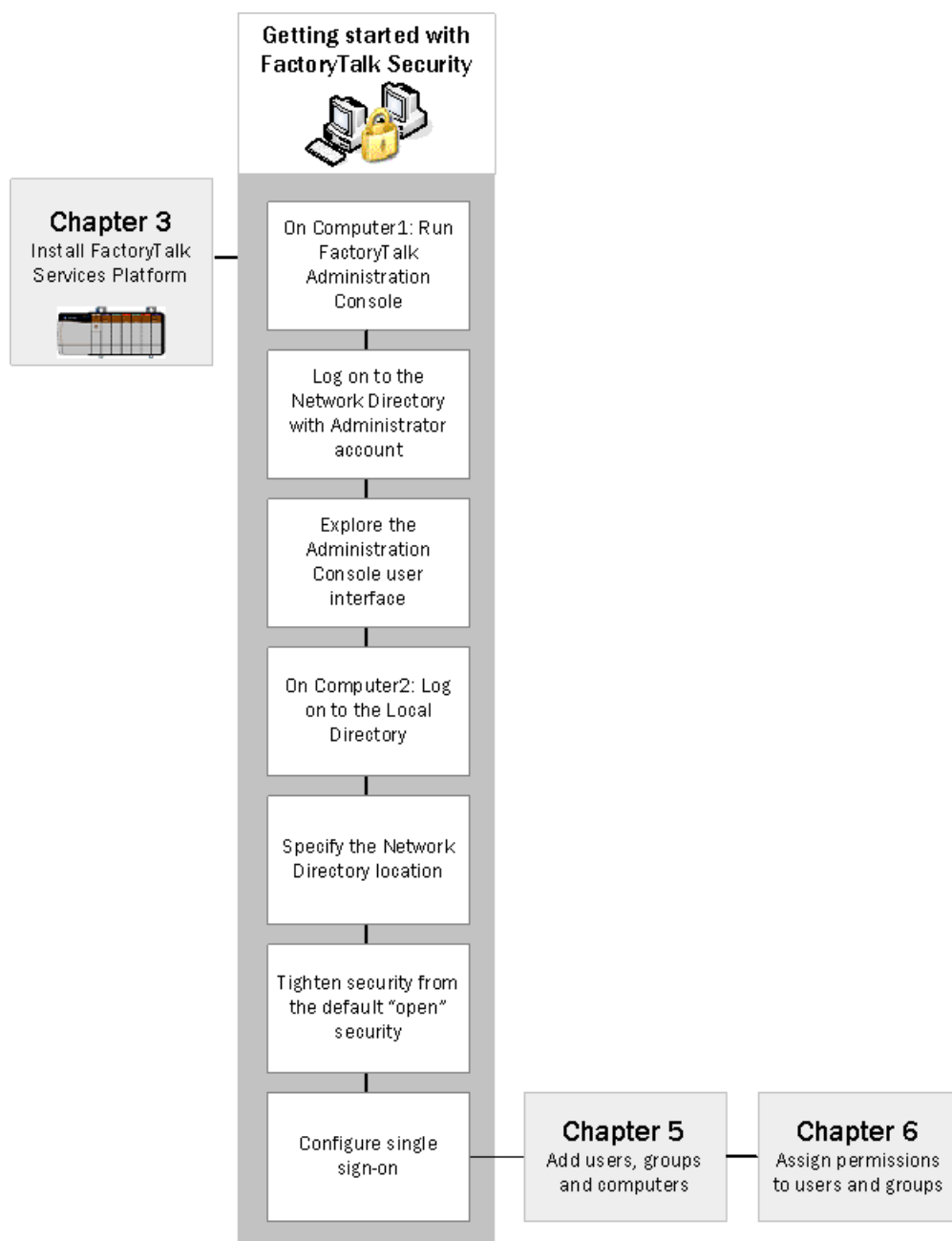
This chapter introduces you to key parts of FactoryTalk Security, including:

- FactoryTalk Administration Console
- Action groups
- Policies
- Computers and groups
- Networks and devices
- Users and groups
- Single sign-on
- Tightening security
- Verify that you have installed and activated the software listed below under [What you need](#) on [page 37](#).
- Become familiar with the terms and concepts of FactoryTalk Security. See [Understanding automation security](#) on [page 17](#) and [About the FactoryTalk system](#) on [page 21](#) for more information.
- FactoryTalk Services Platform v. 2.10 (CPR 9) or later. Using the newest available version is recommended.
- FactoryTalk Security (installed with FactoryTalk Services Platform)

Before you begin

What you need

Follow these steps



Opening FactoryTalk Security

FactoryTalk Security is not a separate product – it is fully integrated into the FactoryTalk Directory – you will not find it on the **Start** menu, or in the **Add or Remove Programs** list in Control Panel.

To get started using FactoryTalk Security, open the FactoryTalk Administration Console: **Start > All Programs > Rockwell Software > FactoryTalk Administration Console** and then log on to the FactoryTalk Local or Network Directory.

Log on to FactoryTalk using an administrator account

To secure your FactoryTalk system, you must log on to that directory using a user account that has administrative access to the directory.

If you installed FactoryTalk Services Platform, version 2.10 (CPR 9) or later on a new computer, you can access the:

- Network Directory using any Windows user account that is a member of the Windows Administrators group your local computer
- Local Directory using any Windows user account

You must log on to, and configure security settings for, each directory separately.

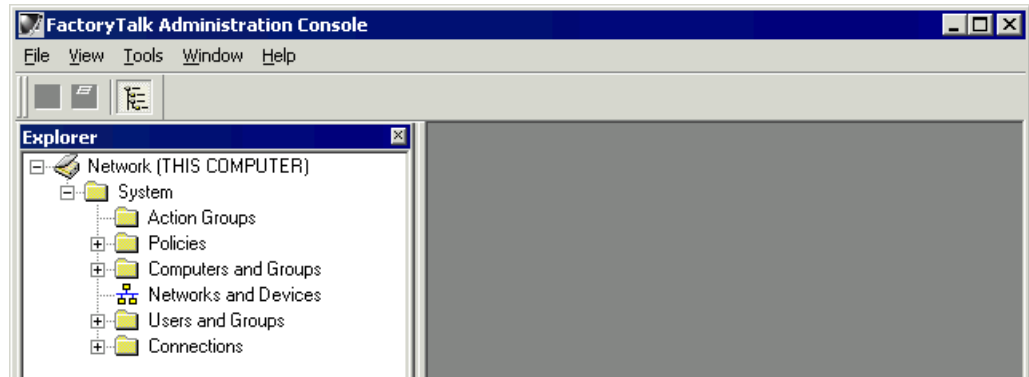
Tip: If the administrator account is a locked or expired Windows-linked account, enable the account in Windows.
If the administrator account is a locked or expired FactoryTalk user account, run the FactoryTalk Directory Configuration Wizard to enable the account. See "Using the FactoryTalk Directory Configuration Wizard" on page 215 for instructions.

FactoryTalk Administration Console

The FactoryTalk Administration Console is your tool for working with FactoryTalk Security. Using this tool, you can:

- browse your FactoryTalk system and view the applications, servers, and devices within it
- create system-wide security settings, and security settings that affect all instances of FactoryTalk-enabled products
- secure the FactoryTalk Network Directory or FactoryTalk Local Directory
- secure resources in your FactoryTalk system, including applications and data

- secure hardware networks and devices



Tip: If you are using FactoryTalk View, you can use either the Factory Talk Administration Console or Factory Talk View Studio to configure security.

The Explorer window

The Explorer window, which is the left pane of the FactoryTalk Administration Console, shows the contents of the FactoryTalk Network Directory or FactoryTalk Local Directory in a tree view.

Use the Explorer window to add and manage security for your FactoryTalk View system (including all security-enabled FactoryTalk products).



Server

The server is the computer hosting the FactoryTalk Directory – either a Network or Local Directory Server.

If you are using a **Network Directory Server**, the term Network appears (as shown above) and the name of the computer appears in brackets. The term "This Computer" indicates that the FactoryTalk Network Directory is on the computer being used. If the Network Directory was being accessed remotely, a computer name would appear in the brackets.

If you are using a **Local Directory Server**, the term Local appears and the name of the computer appears in brackets.

Application

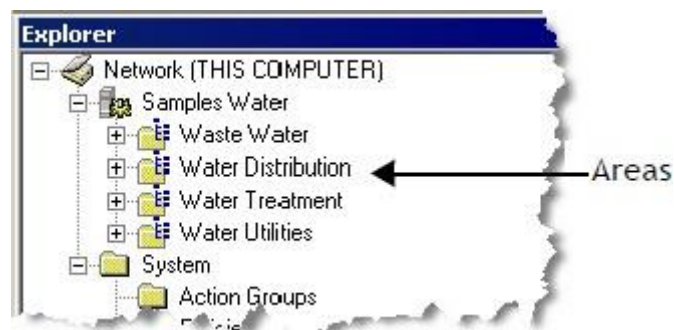
An application organizes project information, including elements such as data servers, HMI servers, and alarm and event servers, and makes that information available to all software products and computers participating in a FactoryTalk system.

Network applications are held in a FactoryTalk Network Directory. Project information and participating software products can be located on multiple computers, distributed across a network. All the computers participating in a particular Network application share a common Network Directory Server located on a network computer.

Local applications are held in a FactoryTalk Local Directory. Project information is located on a stand-alone computer and is available only to software products installed on that same local computer. Local applications cannot be accessed remotely and cannot share project information with a Network application.

Area

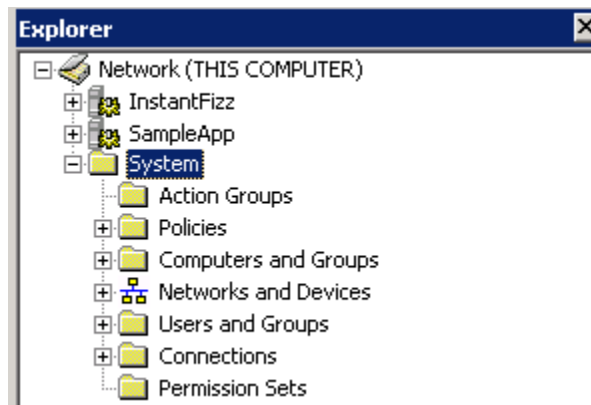
Areas organize and subdivide a distributed Network application into logical or physical divisions. For example, separate areas might correspond with separate manufacturing lines in a facility, separate plants in different geographical locations, or different manufacturing processes.



Areas are not available with Local applications.

System folder

The System folder contains a list of user, computer, and group accounts, passwords, system-wide policy settings, and system-wide security settings. All of the items in the System folder apply to every application in the FactoryTalk Directory.



The items within the System folder are described in more detail on the following pages.

Application and Communications tabs

The tabs at the bottom of the Explorer window are available only if RSLinx Enterprise is installed. The **Application** tab allows you to view the Explorer window. The **Communications** tab allows you to view the control hardware available to the local computer through RSLinx Enterprise.



What you see here is not the same as Networks and Devices. Rather, this is for viewing the control hardware available to the local computer through RSLinx Enterprise.

You'll see these tabs only if RSLinx Enterprise is installed.

If you are running FactoryTalk View Machine Edition, the **Communications** tab displays the same information as the **Design (Local)** tab on the **Communication Setup** dialog box in FactoryTalk View ME. For information, see "Use the Design (Local) and Runtime (Target) tabs on the Communication Setup dialog box (FactoryTalk View Machine Edition)" in RSLinx Enterprise online help.

Action groups (System folder)

Action groups allow you to group actions together and then assign security permissions to all of the actions in the group. This allows you to grant or deny permissions for a set of actions in one step, rather than having to set

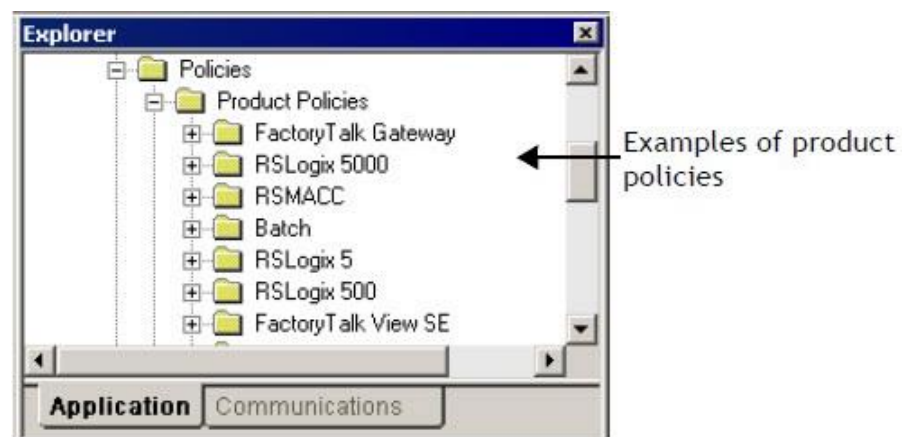
permissions for each action separately.

Create action groups that make sense in your facility. For example, create groups based on:

- a person's role or job (operator, supervisor, engineer, and so on)
- the equipment a person has access to (hoppers, mixers, ovens, and so on)

Policies (System folder)

A policy is a setting that applies across the entire FactoryTalk system. There are two types of policies – Product policies and System policies.



Product policies are sets of securable features for the individual products in your FactoryTalk system. You can define security settings to restrict access to the features of individual FactoryTalk products in your system, and to prevent inadvertent changes, or tampering. Only users with the required level of access can use the product features that you have secured.

The policy information for each FactoryTalk product is preloaded in the FactoryTalk Directory. You can modify these policies on a product-by-product basis for specific users, groups, and computers included within the FactoryTalk Directory.

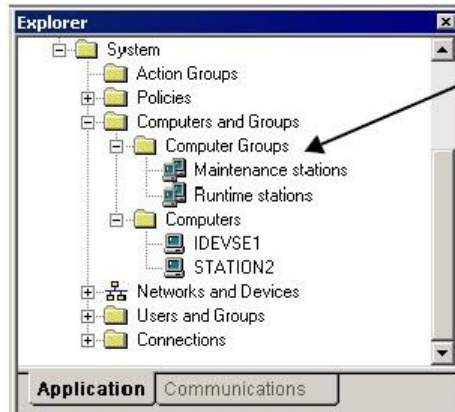
System policies are sets of policies that are system wide. Examples of system policies are:

- **Security** – password length, complexity, expiration, and so on
- **Audit checks** – whether access checks are audited, whether access grants, denies or both are audited, and so on
- **User rights** – whether users can perform certain actions, such as backing up and restoring the contents of the FactoryTalk directory

All FactoryTalk products use the policies in the System Policies folder. When you install individual products, they can add their own policies to the Product Policies folder.

Computers and groups (System folder)

A computer account represents a physical computer on the network. *Computers and Groups* allow you to create computer accounts that determine which computers have access to your FactoryTalk system.



Grouping computers simplifies administration of security permissions. By changing a computer's group memberships, you can quickly change the resources to which the computer has access.

Tip: You can create computer accounts or computer group accounts only in a FactoryTalk Network Directory – not a Local Directory.

Once you have added the computer account, you can specify security settings for the computer – for example, to allow or deny access to parts of the FactoryTalk system from the computer or to configure how long the directory cache files are available after the client is disconnected from the FactoryTalk directory server. You can also add the computer to a group account that includes multiple computers, and then specify security settings for the group. For example, you might use these accounts to enforce line-of-sight security, to ensure that operators control critical or dangerous operations only when they can see the equipment they are operating.

Important: You must create computer accounts for any computers hosting servers — for example, Terminal Servers, Rockwell Automation Device Servers (RSLinx Enterprise), OPC data servers, Tag Alarm and Event Servers, or HMI servers. Without the server computer accounts, you will not be able to configure the servers from client computers on the network because the FactoryTalk Network Directory Server cannot locate these servers on the network without their computer accounts.

This is true even if the security policy called **Require computer accounts for all client machines** is disabled.

Networks and devices (System folder)

Networks and Devices are the control hardware available to the local computer through RSLinx Classic. These control networks and devices can be different for each computer in the system.

You can secure the control hardware accessible through RSLinx Classic either in FactoryTalk Administration Console or RSWho. Security settings configured in RSWho appear in FactoryTalk Administration Console when you right-click **Networks and Devices** and then click **Refresh**. If

Autobrowse is enabled in RSWho, security settings configured in FactoryTalk Administration Console immediately appear in RSWho.

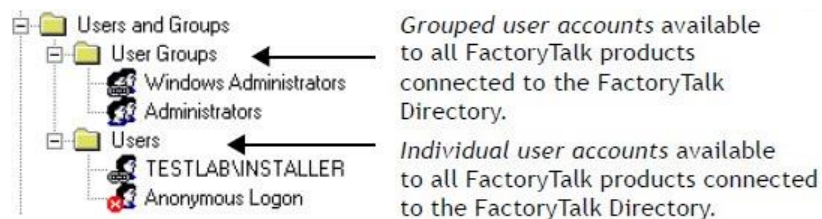
The steps for securing these networks and devices are the same as for any other resource in your FactoryTalk system. However, there is a slightly different set of rules for applying inherited security permissions to control devices secured with logical names.

If you want to secure hardware in "groups", use resource grouping to set up security through the application or area (for Network systems) or through the application (for Local systems). See [Using resource groupings](#) on [page 104](#) for more information.

Users and groups (System folder)

The Users and Groups folder allows you to control who accesses the FactoryTalk system and from which computer. Access can be restricted to a single user or group of users, as well as to a single computer or group of computers.

When setting up security, create groups first and grant the appropriate permissions to the group. This allows you to create a security structure without needing to know exactly who the users will be. When users are added to the group, they inherit the permissions granted to the group. If necessary, you can then deny individual users specific permissions later.



Tip: You can create Windows-linked user accounts that are linked to user accounts that already exist in a Windows domain or workgroup. For details, see FactoryTalk Help.

Specify the Network Directory location

To share FactoryTalk Network Directory services and resources, you must connect the local computer to a FactoryTalk Network Directory Server and participate in the applications that are hosted on that server. To do this, use the FactoryTalk Directory Server Location Utility. (You don't need to do this for a Local Directory on a stand-alone computer.)

To change the location of the Network Directory Server, you must be logged on to the computer with an account that has permissions to change the directory server. For details about the security settings, see [Assigning system policies](#) on [page 96](#).

Run the FactoryTalk Directory Server Location Utility

You can run the utility from the:

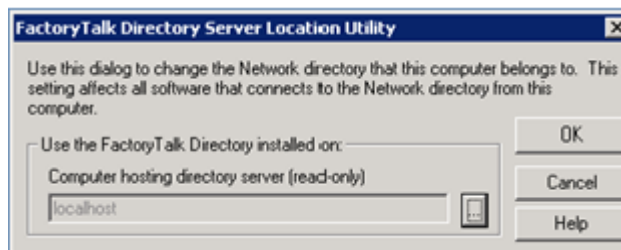
- Windows **Start** menu:
Click **Start > All Programs > Rockwell Software > FactoryTalk Tools > Specify FactoryTalk Directory Location**.
- FactoryTalk Administration Console:
From the **Tools** menu, click **FactoryTalk Directory Server Options**.

Point client computers to the directory server computer

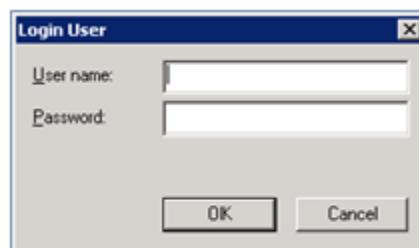
1. On each participating Network Directory client computer, run the FactoryTalk Directory Server Location Utility.

Example: Go to **Computer2**, the client computer we are using for these examples, and run the Directory Server Location utility.

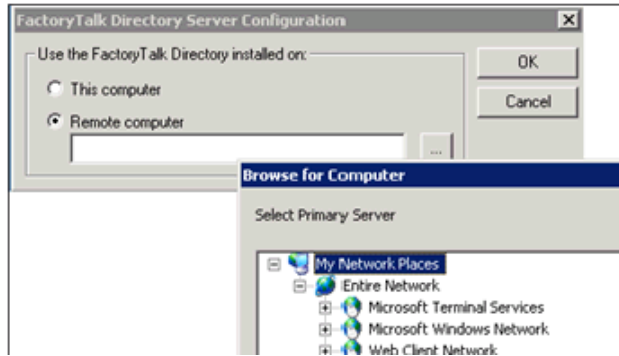
2. In the **FactoryTalk Directory Server Location** dialog box, click the **Browse** button.



3. In the **Login User** dialog box, type the Administrator user name and password, and then click **OK**.



4. In the **FactoryTalk Directory Server Configuration** dialog box, click **Remote computer** and then type or browse for the name of the computer you want to use as the Network Directory Server.



Example: For this example, select the computer referred to as Computer1, where FactoryTalk Activation and FactoryTalk Administration Console are installed.

5. Click **OK**.

When prompted to do so, log on to the new Network Directory Server.

If single sign-on is enabled on the computer when you change the location of the Network Directory Server, the single sign-on session terminates, and you must log on to the new Network Directory Server. The user name and password you enter becomes the new single sign-on credentials for all participating FactoryTalk products on the computer.

Log on to FactoryTalk using a Windows Administrator account

To start securing your FactoryTalk system, you must log on to the FactoryTalk directory using a user account that has administrative access to the directory.

1. Do one of the following to log on to FactoryTalk:
 - On the Windows Start menu, select **Start > All Programs > Rockwell Software > FactoryTalk Tools > Log on to FactoryTalk**.
 - In the notification area of Windows taskbar, double-click the FactoryTalk Directory icon .
 - Log on to a FactoryTalk product and use the same credentials to also automatically log on to the FactoryTalk Directory.
2. In the **Directory** list, select the FactoryTalk Directory you want to log on to:

- Click **Network** to access Network applications on the Network Directory Server.
- Click **Local** to access Local applications on the Local Directory.

Example: For this example, select **Network**.

- If you cannot log on to a particular directory on this computer, it may be because you do not have a valid user account in that directory.
3. Do one of the following:
 - If you are not already logged on to a FactoryTalk Directory, click **Log On**.
 - If you are already logged on to a FactoryTalk Directory and want to log on as a different user, or if you want to log on to a different directory, click **Change Logon**.
 4. In the **Log On** dialog box, type your user name and password, and then click **OK**.
 - If you have the same user name and password for a Windows-linked account and a user account, you can log on to the Windows-linked account deliberately by typing the user name in the format, **DOMAIN\username** in the User Name box.
 - If you have the same user name and password in your computer's local workstation domain and in a Windows network domain, you will be logged on to the same domain that you are currently logged on to in Windows, unless you specify the name of the domain.

Security settings are separate in the Network and Local Directory

Security settings are stored in the FactoryTalk Directory. The FactoryTalk Network Directory and FactoryTalk Local Directory are completely separate and independent of each other. User accounts, passwords, security permissions, system-wide policy settings, and project information are completely separate and cannot be shared between the Network Directory and the Local Directory. Configuring any of these items in one directory does not configure them in the other. Similarly, changing the password to a user account in one directory does not change the password the other directory, even if the account has the same name in both directories.

Tip: All the computers participating in a particular FactoryTalk View application share a common FactoryTalk Directory located on a network computer.

Important: The FactoryTalk Directory server must not be installed on the same computer as the domain controller for the network.

Securing the actions users can perform

FactoryTalk Directory Configuration Wizard

If an error occurred while you were installing the FactoryTalk Services Platform, or you are upgrading from a previous version of FactoryTalk Automation Platform, you may have to manually configure the FactoryTalk Directory by running the FactoryTalk Directory Configuration Wizard. Refer to Using the FactoryTalk Directory Configuration Wizard for more information on when to run the FactoryTalk Directory Configuration Wizard.

When setting up security, you can specify which actions a user or group can perform on the resources in your system while working from a particular computer or group of computers. In a FactoryTalk Local Directory, actions can only be performed from the local computer — the FactoryTalk Local Directory does not contain any computer accounts.

Differences between securable actions and product policy feature security

In addition to securing actions users can perform, you can define product policies that determine what features a user can access in various FactoryTalk products. See *Differences between securable actions and product policy features* and *Secure product policy features* in the FactoryTalk Security Help (*\Program Files\Common Files\Rockwell\Help\FTSecurityEN.chm*).

Action groups

You can group actions together and then assign security permissions to all of the actions in the group. See *About action groups* in the FactoryTalk Security Help.

Default securable actions

This section lists the securable actions, organized by category, that are installed by default with the FactoryTalk Services Platform. However, different sets of actions apply to different resources in the directory.

Important: Additional securable actions might appear, depending on which FactoryTalk products you have installed. For details about using those actions, see the documentation for your FactoryTalk products.

To secure the actions for a particular resource:

1. In FactoryTalk Administration Console or FactoryTalk View Studio, in the Explorer window, right-click the resource you want to secure, and then click **Security** on the pop-up menu.

2. Specify permissions for the following actions and then click **OK**.

RSLink Enterprise actions

See RSLink Enterprise Help: From the help **Contents** tab, open the book **Work with RSLink Enterprise > Secure RSLink Enterprise using FactoryTalk Security**, and then open the topic *How to specify FactoryTalk Security permissions to enable you to perform RSLink Enterprise tasks*.

FactoryTalk Transaction Manager actions

See FactoryTalk Transaction Manager Online Help: From the help **Contents** tab, open the book **Secure FactoryTalk Transaction Manager using FactoryTalk Security**, and then open the topic *Specify FactoryTalk Security permissions that allow you to perform FactoryTalk Transaction Manager tasks*.

RSLogix 5 actions

These actions are available from the Networks and Devices tree and apply to all of the control hardware listed in the tree. These actions apply only to the RSLogix 5 software product.

See the *RSLogix 5 Getting Results Guide*.

RSLogix 500 actions

These actions are available from the Networks and Devices tree and apply to all of the control hardware listed in the tree. These actions apply only to the RSLogix 500 software product.

See the *RSLogix 500 Getting Results Guide*.

RSLogix 5000 actions

These actions are available from the Networks and Devices tree and apply to all of the control hardware listed in the tree. These actions apply only to Logix Designer application.

See the *Logix Designer application Help*.

FactoryTalk Batch actions

See FactoryTalk Batch Administrator's Guide: From the Windows **Start** menu, click **Start > All Programs > Rockwell Software > FactoryTalk Batch Suite > Online Books > FactoryTalk Batch > Batch Administrator's Guide**.

Common actions

Read

Controls whether a user or group can see the resource in the Explorer window from a computer or group of computers.

- **For the Network Directory or Local Directory**, denying Read prevents users from seeing the directory or its contents.
- **For an application**, denying Read prevents users from seeing the application or its contents. Denying Read does not prevent users from reading tag values from data servers in the application.
- **For an area**, denying Read prevents users from seeing the area or its contents. Denying Read does not prevent users from reading tag values from data servers in the area.
- **For the System folder**, denying Read prevents users from seeing the System folder or its contents. Denying Read does not prevent users from reading tag values for devices in the Networks and Devices tree.
- **For the Networks and Devices tree in the System folder**, denying Read prevents users from seeing the Networks and Devices tree and its contents. Denying Read does not prevent users from reading tag values for a particular device.
- **For an individual network or device** within the Networks and Devices tree, denying Read prevents users from seeing the network or device and its contents. Denying Read does not prevent users from reading tag values for a particular device.

Important: Take care when explicitly denying Read and List Children rights — many applications require common Read and List Children rights to allow access to security rights. If the various applications cannot read their security rights, the application will either not run, or will run with limited functionality.

Write

Controls whether a user or group can write to the resource from a computer or group of computers.

- **For the Network Directory or Local Directory**, denying Write prevents users from modifying the properties of any item in the directory. For example, denying Write prevents users from modifying the description of an application, area, or the properties of a data server. However, if Create Children is allowed, the user or group can create applications in the directory, add areas to an application, and add data servers to areas.

- **For an application**, denying Write prevents users from modifying the properties of any item in the application. For example, denying Write prevents users from modifying the description of the application, the descriptions of areas within the application, or the properties of data servers within the application or its areas. However, if Create Children is allowed, the user or group can add areas or data servers to an application, and can add data servers to areas.
- **For an area**, denying Write prevents users from modifying the properties of any item in the area. For example, denying Write prevents users from modifying the description of the area, or the properties of data servers within the area. However, if Create Children is allowed, the user or group can add areas or data servers within the area.
- **For the System folder**, denying Write prevents users from modifying the properties of any item in the System folder. For example, denying Write prevents users from modifying policy settings, and the properties of user accounts, such as an account's description or group memberships. Denying Write also prevents deleting user and group accounts, if the accounts have group memberships associated with them. This is because the group memberships are updated automatically when an account is deleted, and updating group memberships is controlled by the Write action.
- **For the Networks and Devices tree in the System folder**, denying Write prevents users from defining or undefining logical names for networks or devices. Denying Write does not prevent users from writing tag values to devices.
- **For an individual network or device** within the Networks and Devices tree, denying Write prevents users from defining or undefining logical names for the network or device. Denying Write does not prevent users from writing tag values to devices.

Configure Security

Controls whether a user or group can change the security permissions for the resource, while working from a computer or group of computers, by clicking **Security** on the pop-up menu.

Denying Configure Security has the same effect on all types of securable resources. For example, if a user is denied Configure Security for an area, the user cannot change the security settings of the area, such as allowing or denying users permission to perform actions in the area, while working from the specified computer or group of computers.

Similarly, denying Configure Security on the Users and Groups folder prevents users from setting security permissions for the Users and Groups folder. Denying Configure Security on the Users and Groups folder does not limit the access users have to resources in the system.

Create Children

Controls whether a user or group can create a new, related resource beneath an existing resource in the directory tree while working from a computer or group of computers.

- **For the Network Directory or Local Directory**, denying Create Children prevents users from creating applications, areas, or servers.
- **For an application**, denying Create Children prevents users from creating areas or servers in the application.
- **For an area**, denying Create Children prevents users from creating areas or servers in the area.
- **For the System folder**, denying Create Children prevents users from creating user, computer, or group accounts. Denying Create Children has no effect on policies.
- **For the Networks and Devices tree**, and for individual networks or devices within the Networks and Devices tree, Create Children is not available because users cannot add items to the Networks and Devices tree. Networks and Devices is populated automatically, based on the networks and devices that are available to your local computer.

List Children

Controls whether a user or group can list the children of the resource from a computer or group of computers.

Denying List Children has the same effect on all types of securable resources. For example, if List Children access is denied to an application, the user or group can see the application, but not its contents while working from the specified computer or group of computers.

Unlike the Read action, List Children does allow the user to see the resource that contains other resources, for example, the application that contains areas or servers.

Execute

Controls whether a user or group can perform an executable action from a computer or group of computers. The Execute action is used primarily for Product Policy Feature Security settings. For details about securing features, see Secure product policy features.

Instead of using the Execute action, each FactoryTalk product can use its own actions to secure its executable features. For details about what, if anything, the Execute action does in a particular FactoryTalk product, see documentation for that product.

Delete

Controls whether a user or group can delete the resource, while working from a particular computer or group of computers.

- **For the Network Directory or Local Directory**, denying Delete prevents users from deleting any item in the directory, for example, applications, areas, servers, or user accounts.
- **For an application**, denying Delete prevents users from deleting the application, or any item within it, for example, areas, or servers.
- **For an area**, denying Delete prevents users from deleting the area, or any item within it, for example, servers within the area.
- **For the System folder**, denying Delete prevents users from deleting any item in the System folder, for example, user, computer, or group accounts. If a user, computer, or group account has group memberships associated with it, deleting the account also requires Write permission, because updating the group memberships of accounts is controlled by the Write action.
- **For the Networks and Devices tree** in the System folder, and for individual networks or devices within the Networks and Devices tree, the Delete action is not available because users cannot remove items from the Networks and Devices tree. Networks and Devices is populated automatically, based on the networks and devices that are available to your local computer.

Tag actions

Write Value

Controls whether a user or group can write to tags in data servers from a computer or group of computers. This action can be configured on the Network Directory or Local Directory, an application, or an area.

The Write Value action does not prevent users from writing values to tags in specific hardware devices. Write Value prevents writing values to all of the tags managed by a data server.

If you have additional FactoryTalk products installed, they might install additional Tag actions. For details about these actions, see Help for your FactoryTalk products.

User action groups

This category contains the action groups you have added. If you have not added any action groups, this category does not appear. For details about action groups, see "About action groups" in the FactoryTalk Security Help.

Tightening security

When you install the FactoryTalk Services Platform on a computer for the first time – rather than upgrading from a previous version – the FactoryTalk Network Directory and the FactoryTalk Local Directory are configured to allow access to all users by default. However, by default, user accounts have slightly different levels of access in the Network Directory and Local Directory.

Because the Network Directory and Local Directory are separate, you must secure them separately.

On a new system

If you installed the FactoryTalk Services Platform software for the first time and all computers participating in the system are using only FactoryTalk Services Platform, version 2.10 (CPR 9) or later:

- In the FactoryTalk Network Directory, all users who successfully log on to Windows **on any local computer** connected to the FactoryTalk Network Directory have full access to the distributed FactoryTalk system on the network
- In the FactoryTalk Local Directory, any user who successfully logs on to Windows on the local computer has full access to the FactoryTalk system on the local computer

Tighten security on a new system:

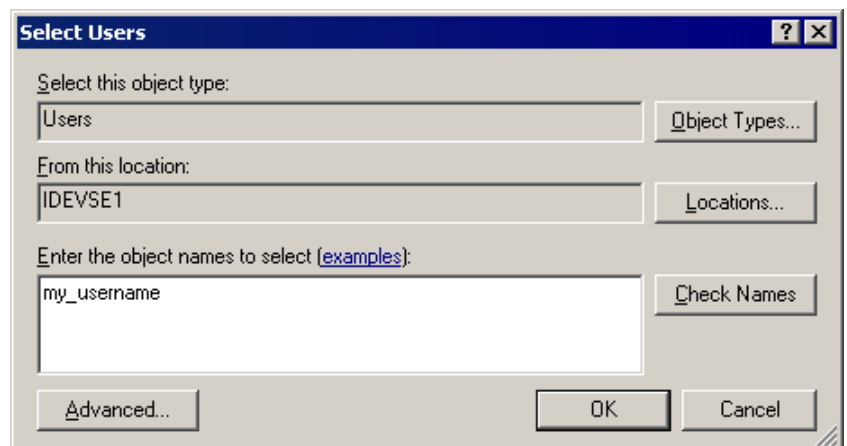
These instructions are for use on a system where FactoryTalk Services Platform has been installed for the first time.

1. Decide which FactoryTalk Directory you want to configure for tightened security. If you need to tighten security in both the Network Directory and Local Directory, choose one, complete the steps below, and then repeat these steps for the other directory.
2. Log on to Windows using an account that is a member of the Windows Administrators group on the local computer (**Computer1** for this example).
3. Start FactoryTalk Administration Console, and then log on to the FactoryTalk Network Directory where you want to tighten security.

From the Windows **Start** menu, click **Start > All Programs > Rockwell Software > FactoryTalk Administration Console**.

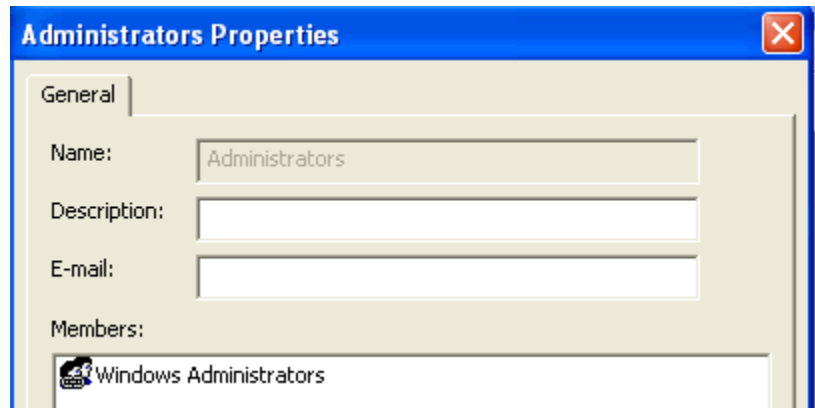
4. To ensure that you always have administrative access to the FactoryTalk Directory, create one or more FactoryTalk user accounts or Windows-linked user accounts. You will add these accounts to the Administrators group in the next step:
 - In the Explorer window, expand **System > Users and Groups > Users**. Right-click **Users**, point to **New**, and then click **User** or **Windows-Linked User**.
 - If you are creating a user account, in the **New User** dialog box, type a user name and password for the account. For help with the other options in the dialog box, click the **Help** button in the dialog box.
 - If you are creating a Windows-linked user account, in the **New Windows-Linked User** dialog box, click **Add**. In the **Select Users** dialog box, type the names of one or more Windows-linked accounts you want to link to and then click **OK**, or click **Advanced** and then click **Find Now** to search for the accounts. When you are finished in the **New Windows-Linked User** dialog box, click **Create**.

Example: For this example, add yourself as a Windows-linked user.



5. Add the user accounts you created in the previous step to the Administrators group:
 - In the Explorer window, expand **System > Users and Groups > User Groups**. Right-click the Administrators group, and then click **Properties** on the pop-up menu.
 - In the **Administrators Properties** dialog box, click **Add**. In the **Select User or Group** dialog box, click **Show users only**, select the user accounts you want to have administrative access, and then

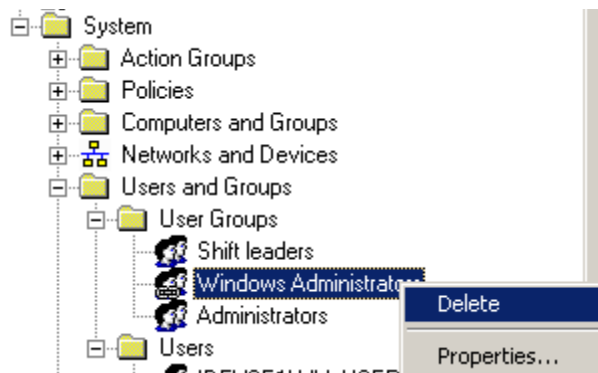
click **OK**. Click **OK** to close the **Administrators Properties** dialog box for the account.



6. Log off FactoryTalk:
 - On the **File** menu, click **Log Off**.
7. Log on to the FactoryTalk Network Directory you are configuring – use the administrator user name and password that you created in step 4.
8. Restrict access to each FactoryTalk Directory. In the FactoryTalk Network Directory and the FactoryTalk Local Directory, remove the Windows-linked groups called Windows Administrators and Authenticated Users.

Note: Be sure you have created an administrator user and added that user to the Administrators group for both the Network and Local Directories — not the Windows Administrators group.

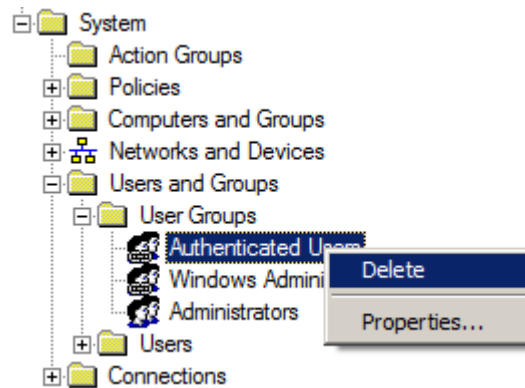
- In the Explorer window, expand **System > Users and Groups > User Groups**. Right-click **Windows Administrators** and then click **Delete** on the pop-up menu.



Removing the Windows Administrators group from the Administrators group prevents all users who are members of the Windows Administrators group **on any local computer** connected

to the FactoryTalk Network Directory from having administrative access to the directory.

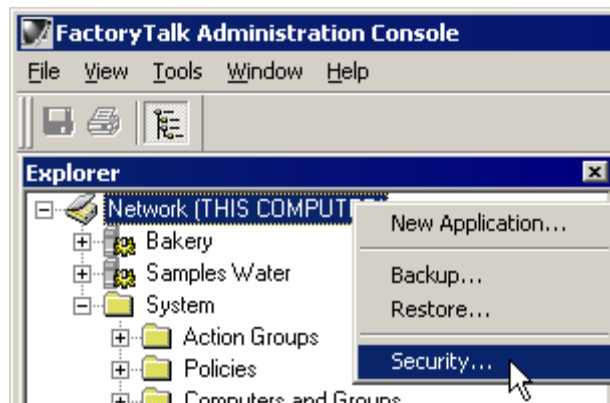
- In the Explorer window, expand **System > Users and Groups > User Groups**. Right-click **Authenticated Users** and then click **Delete** on the pop-up menu.



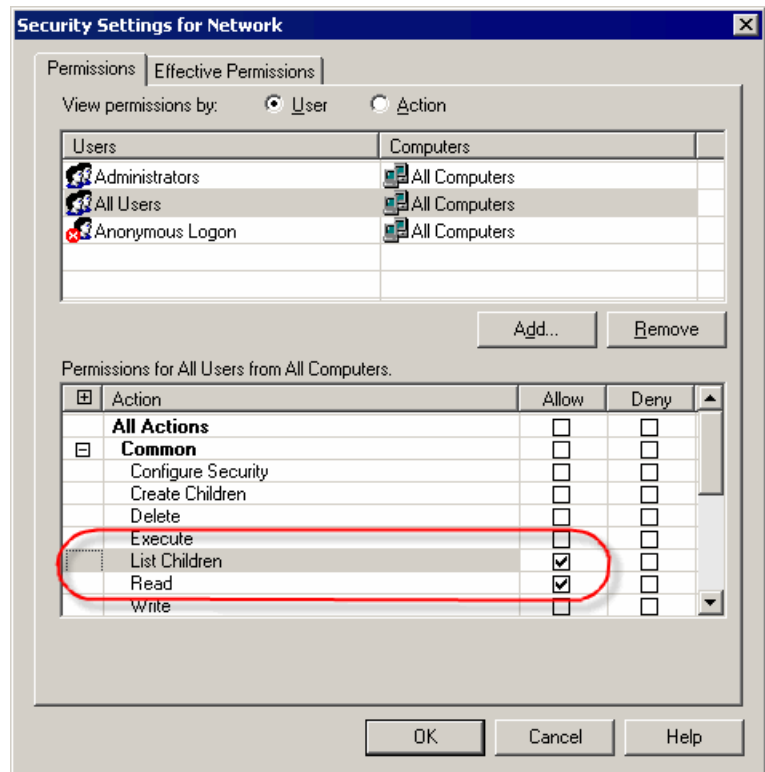
Deleting the Authenticated Users group prevents all user accounts that have successfully logged on to Windows **on any local computer** connected to the FactoryTalk Network Directory from having access to the directory.

9. Restrict access to **All Users**:

- At the top of the Explorer window, right-click **Network** or **Local**, and then click **Security** on the pop-up menu.



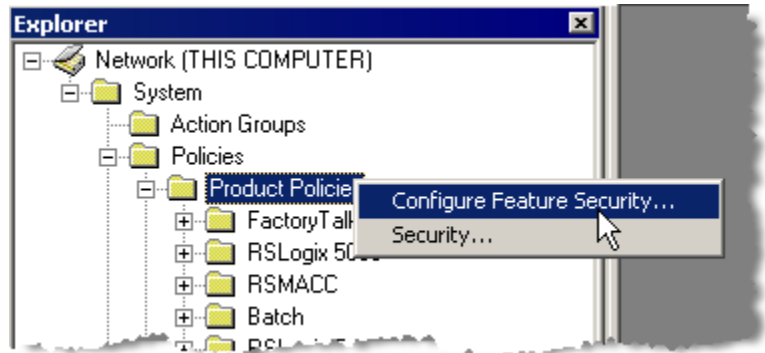
- On the **Permissions** tab, select **All Users**.
- In the **Permissions** list, beside **All Actions**, clear the **Allow** and **Deny** check boxes.
- Expand the **Common** group of actions, and then select the **Allow** check boxes for **Read** and **List Children**.



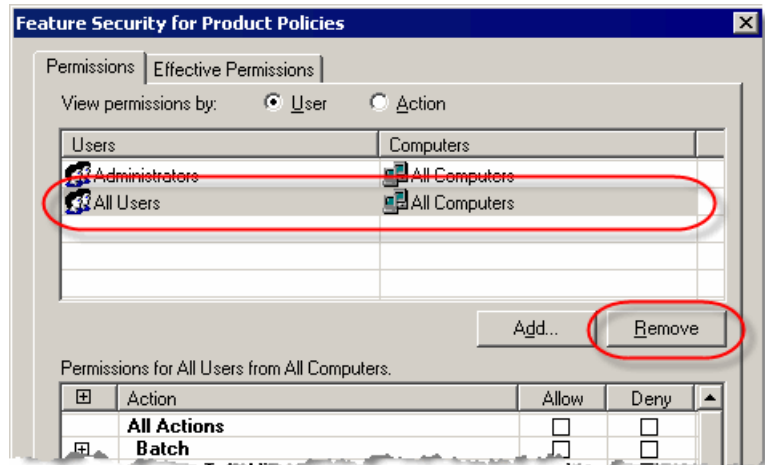
10. Remove **All Users** from product policies:

The last step for reducing rights to the **All Users** group is to remove the rights granted to All Users in the Product Policies.

- From the Explorer window, expand the FactoryTalk Directory as shown and locate the Product Policies folder.
- Right-click **Product Policies**, and then click **Configure Features Security** on the context menu.



- On the **Feature Security for Product Policies** dialog box, select **All Users**, and then click the **Remove** button.



The All Users group is removed from the FactoryTalk Directory and all permissions that were set for that group are deleted.

11. Next, secure your system policy settings, which define general rules for implementing security across all FactoryTalk products in your system. For details about securing policies, see [Setting up system-wide policies and product policies](#) on [page 93](#).

Once you have set this basic level of security, create user groups and user accounts for those users that need greater access to the system, and then configure security for those accounts.

On an upgraded system

If you upgraded an existing FactoryTalk system from FactoryTalk Automation Platform version 2.00, your security system will continue to work as it did before, so you might not need to tighten security any further.

However, during the upgrade, if a valid (not disabled or expired) FactoryTalk administrator account could not be found in the FactoryTalk Network Directory or FactoryTalk Local Directory, you cannot log on to the directory and you must run the FactoryTalk Directory Configuration Wizard manually after installation. Running the wizard manually **the first time** gives full access to all users **on any local computer** that is connected to the FactoryTalk Network Directory. To tighten security in your system, you must revoke this access manually. For more information on tightening security on an upgraded system, see [Tightening security](#) on [page 55](#).

Logging on and off with single sign-on

Once a user has logged on to the FactoryTalk system once, any actions requiring the same level of security are permitted in other FactoryTalk products on the same computer, without the need for the user to log on to each product separately. This is a security policy called **single sign-on**, and is defined by the system administrator. Single sign-on is enabled by default.

For example, suppose that single sign-on is enabled, and user called Jane has a Windows-linked account. Jane can log on to the system once, and is not prompted to log on again when she runs FactoryTalk View SE Client, FactoryTalk View Studio, RSLogix, and so on, on that same computer.

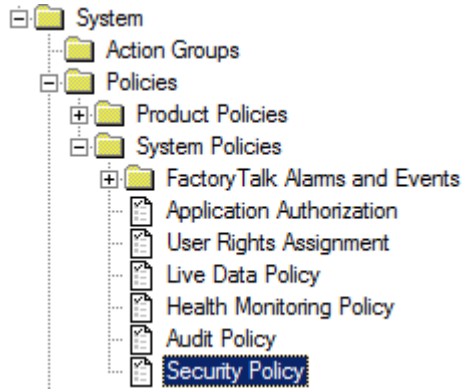
When single sign-on is enabled:

- If Jane has a FactoryTalk user account, she would log on to Windows, and then log on to FactoryTalk. Once logged on to FactoryTalk, she would not be prompted to log on again when she runs another FactoryTalk product that allows single sign-on.
- If Jane has a Windows-linked account, she would log on to Windows, select the Network Directory or Local Directory, and then be automatically logged on to FactoryTalk using her Windows-linked account. She would not be prompted to provide a user name and password at all. Once logged onto FactoryTalk using her Windows-linked account, she would not be prompted to log on again when she runs another FactoryTalk product that allows single sign-on.

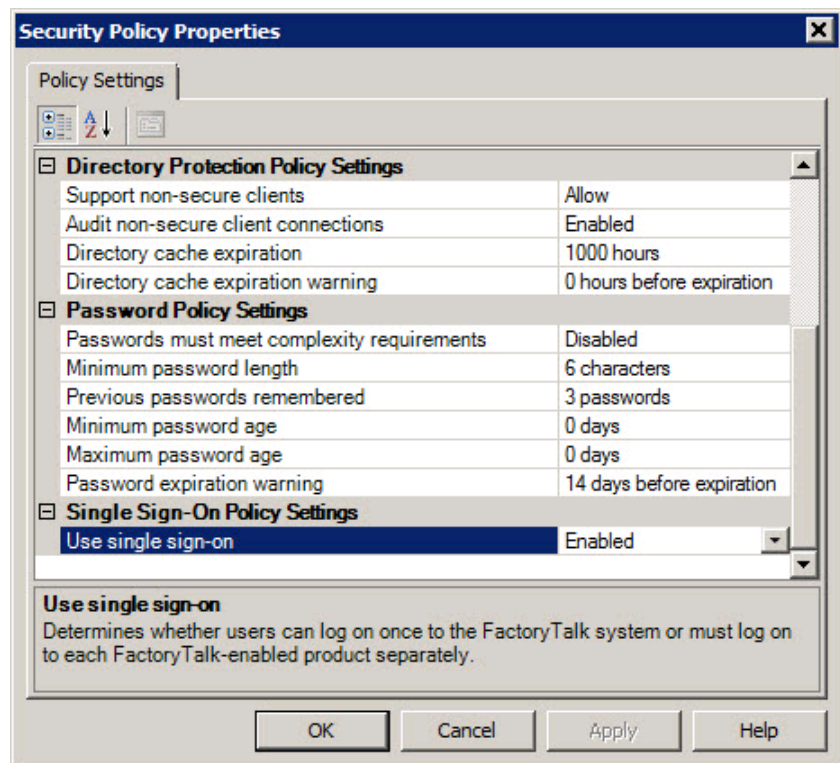
Setting up single sign-on

Single sign-on is a security policy setting. To set it up:

1. In the FactoryTalk View Studio Explorer window, open the **System** folder, open **Policies > System Policies**, and then double-click **Security Policy**.



2. In the **Single Sign-On Policy Settings** list, verify whether **Use single sign-on** is enabled or disabled.



If single sign-on still does not seem to be working properly, it is likely that the FactoryTalk product you are using does not support the single sign-on capability. Some FactoryTalk products always require users to log on, even if single sign-on is enabled.

For detailed information on using single sign-on, see FactoryTalk Help.

Two ways to log on

You can log on to FactoryTalk in one of two ways:

- From the Windows Start menu – to log on to FactoryTalk, you can run **Start > Programs > Rockwell Software > FactoryTalk Tools > Log On to FactoryTalk**.

Once you select the Network Directory or Local Directory and then log on with a user account, all subsequent attempts to access FactoryTalk products from this same FactoryTalk Directory and this same computer automatically use this same user name and password, if single sign-on is enabled. If single sign-on is disabled, users are always prompted to provide credentials when logging on.

- From a FactoryTalk product – if you log on to a FactoryTalk product without first logging on to FactoryTalk, then security uses this user name and password to also automatically log on to the FactoryTalk system. All subsequent attempts to access FactoryTalk products, from this same FactoryTalk Directory on this same computer, automatically use this same user name and password, if single sign-on is enabled.

For example, suppose Jane has a user account and logs on to FactoryTalk Administration Console with the user name "Jane" and the password "robotics." Behind the scenes, security uses this same name and password to silently log Jane on to the FactoryTalk system. If Jane later runs FactoryTalk View, the system uses her security credentials and allows her to access the product without prompting her to log on again, even if she has closed or logged off from FactoryTalk Administration Console.

Logging on as administrator with single sign-on

If a computer is being used by multiple users, one of whom is an administrator, the administrator should be careful that the administrator account does not remain logged on as the single sign-on account, because all subsequent FactoryTalk products that run on the computer will automatically use the administrator account.

Administrators should log on to FactoryTalk using a non-administrator account, and then log on to individual FactoryTalk products as administrator. This allows administrators to make changes without changing the single sign-on user.

Two ways to log off

While you can log on to FactoryTalk from either the Windows Start menu or automatically as part of logging on to a FactoryTalk product, you must use the **Log On to FactoryTalk** tool to log off from the FactoryTalk system.

- If you log off a FactoryTalk product, such as FactoryTalk Administration Console or FactoryTalk View, from the product's File menu, and do not log off FactoryTalk using the Log On to FactoryTalk tool, you remain logged on to FactoryTalk, and all subsequent attempts to access FactoryTalk products automatically use the user name and password shown in the Log On to FactoryTalk tool.
- If you log off FactoryTalk using the Log On to FactoryTalk tool, but do not log off from the product's File menu, you remain logged on to any FactoryTalk products, but you are prompted for a user name and password the next time you run a FactoryTalk product on this computer. If single sign-on is enabled, all subsequent attempts to access FactoryTalk products then use that same user name and password. If single sign-on is disabled, users are always prompted to provide credentials when logging on.

For example, suppose Jane logs on to the FactoryTalk Administration Console with the user name "Administrator" and then later logs off from the Administration Console's File menu. While Jane is out to lunch, Joe uses the computer to run FactoryTalk View. When he starts up the software, he is not prompted to log on, because Jane's "Administrator" account is still logged on to the FactoryTalk system. Joe now has Jane's "Administrator" security rights in every FactoryTalk product he runs, until the computer logs off Windows or until the Log On to FactoryTalk tool logs off "Administrator."

When to disable single sign-on

If multiple users are sharing the same Windows user account, but have different FactoryTalk Security user accounts, it might be necessary to disable single sign-on. This is because with single sign-on enabled, the last user that logged on to FactoryTalk is automatically logged on to all subsequent FactoryTalk products. If you need to be able to distinguish the actions of individual users, disable single sign-on to force all users to identify themselves to each FactoryTalk product they use.

There is no way to log all users off all FactoryTalk products simultaneously. This is because some products might need to run without interruption in the background. To log all users off all FactoryTalk products simultaneously, log off Windows. Logging off Windows also shuts down all FactoryTalk products that were started in the Windows session, regardless of how many users were logged on.

Where to go from here

Do one of the following:

- Go to [Creating user accounts](#) on [page 67](#) to learn about creating user, group, and computer accounts.
- Go to [Assigning permissions](#) on [page 79](#) to learn about assigning permissions to the users, groups, and computers added in this chapter.
- Go to [Setting up system-wide policies and product policies](#) on [page 93](#) to learn about setting system-wide and policy-wide security policies.
- Go to [Resource grouping](#) on [page 103](#) to learn about FactoryTalk Security advanced features, such as resource grouping.
- Go to [RSLinx and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLinx software.
- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure projects and devices like Logix5000, PLC, and SLC controllers.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components
- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.

Creating user accounts

User accounts allow you to control who accesses the FactoryTalk system and from which computer. Access can be restricted to a single user or group of users, as well as to a single computer or group of computers.

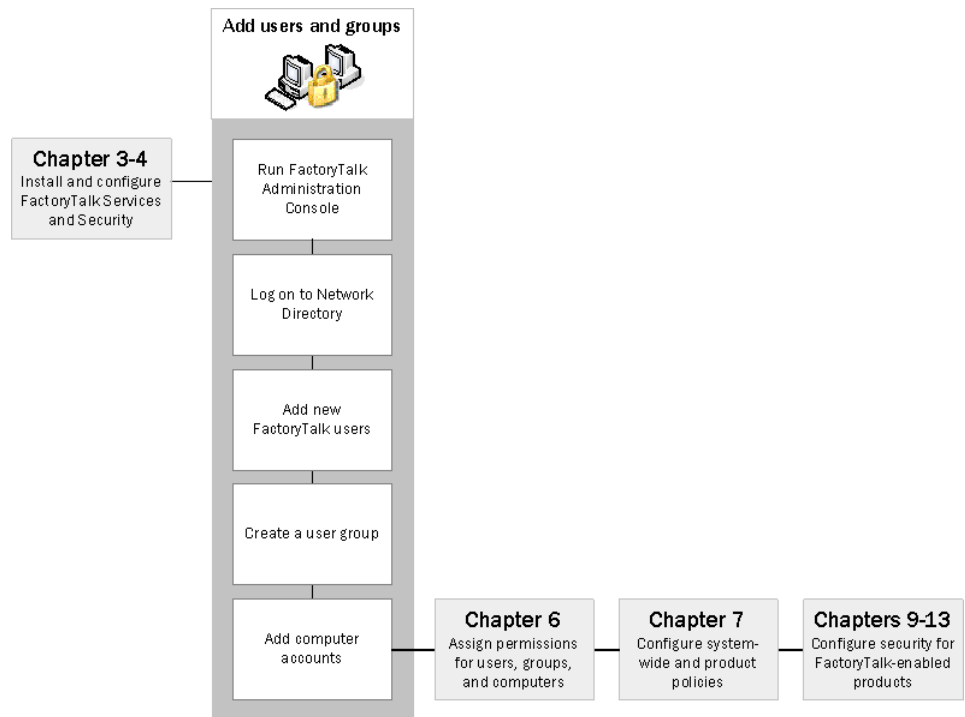
This chapter describes how to create user accounts, including information about:

- Network and Local user accounts
- FactoryTalk user accounts and Windows-linked user accounts
- Planning your accounts
- A simple scenario that shows the process of setting up a user accounts in a FactoryTalk security system
- Verify that you have installed and activated the software listed below under [What you need](#) on [page 67](#).
- Verify that you have configured the Network Directory as discussed in [Specify the Network Directory location](#) on [page 45](#).
- Become familiar with the terms and concepts of FactoryTalk Security. See [Understanding automation security](#) on [page 17](#) and [About the FactoryTalk system](#) on [page 21](#) for more information.
- FactoryTalk Services Platform v. 2.10 (CPR 9) or later. Using the newest available version is recommended.
- FactoryTalk Security (installed with FactoryTalk Services Platform)

Before you begin

What you need

Follow these steps



FactoryTalk user accounts and Windows-linked user accounts

You can add FactoryTalk user or group accounts, FactoryTalk temporary user accounts, or Windows-linked user or group accounts to your FactoryTalk system.

- FactoryTalk user or group accounts

These accounts are separate from the user's Windows account. This allows you to specify the account's identity (for example, the user name), set up how the account operates (for example, whether the password expires), and specify the groups the account belongs to.

- FactoryTalk Temporary User

Use this type of user account if you want to allow users to temporarily utilize the privileges of another user in a different group. This involves creating a special temporary user account, defining who is permitted to authorize the use of this account, and the use of a challenge and response scheme for generating the password for the account.

The user requesting access and the user authorizing access must be in the same FactoryTalk Directory. Both users must be connecting to the FactoryTalk Directory or using cached directory. If using cached directory, make sure it contains the temporary user account.

To use this type of user account:

- a. Create a temporary user account

Temporary User accounts can be added to groups in the same way as other types of user accounts. Their security privileges are also defined in the same way as other types of accounts. For more information about how to configure the duration for temporary passwords and groups granting temporary passwords, refer to FactoryTalk Security Help.

b. Request a temporary password

At the computer where the use of the Temporary User account is needed, in FactoryTalk Administration Console, select **Tools > Temporary Password > Request**. For more information, see FactoryTalk Help.

c. Authorize a temporary password

At the computer where the use of the Temporary User account will be authorized, in FactoryTalk Administration Console, select **Tools > Temporary Password > Authorize**. For more information, see FactoryTalk Help.

d. Use a temporary password

After being authorized, the generated password can be used to log in with the Temporary User account on the computer where password is requested.

Tip: A password requested on one computer will not work on any other computer. The password only can be used until it expires.

- Windows-linked user or group accounts

These accounts are managed by Windows. A Windows-linked user account is linked to the user's Windows account. Add Windows-linked user accounts from a Windows domain or workgroup to the FactoryTalk system to allow the user accounts in the group to access the FactoryTalk system. You cannot change any Windows-linked account information, but you can change the groups the user belongs to.

Tip: Adding Windows-linked accounts to FactoryTalk means you maintain only one security system.

A Windows-linked user or Windows-linked user group is a user/user group account whose credentials are managed and authenticated by the Windows operating system, but linked into the FactoryTalk Security services.

The Windows-linked user group Windows Administrators account is added to the FactoryTalk Administrators group, giving full access to

the FactoryTalk Network Directory to all Windows user accounts that are members of the Windows Administrators group on any local computer connected to the FactoryTalk Network Directory. You can remove this level of access after installation. See [Tightening security on page 55](#).

The Windows-linked user group account **Authenticated Users** is added to the FactoryTalk Network Directory and FactoryTalk Local Directory if you install the FactoryTalk Services Platform on a new computer. You can remove this level of access after installation. See [Tightening security on page 55](#).

During installation, the **\$AnonymousLogon** user account is created automatically and is given Common/Read and Common/List Children access to the FactoryTalk Network Directory and FactoryTalk Local Directory. This account is used after installation when FactoryTalk products require service access to the directory.

Tip: Create FactoryTalk user and group accounts and add your Windows-linked users and groups to them. This allows you to assign rights to the FactoryTalk user and group accounts and not the Windows-linked accounts. This is especially important if you are going to be switching from a development domain to a production domain — only the Windows-linked accounts have to be updated.

Planning your accounts

When planning your accounts, follow the best practice below.

Tip: As much as possible, create group accounts rather than individual user accounts. This simplifies administration, and allows you to secure resources in your system by defining security permissions for the group accounts before all the individual user and computer accounts have been created. You can then add user and computer accounts to the groups at any time, and all of the individual accounts in the groups will have the security settings of those groups.

Where to start

To plan security for your system:

- Make lists of users.
- Divide the users into groups.
- Plan which resources users need to access.

Scenario for securing parts of a system

- Plan which actions users will be allowed to perform on those resources and from which computers or groups of computers.

Imagine a simple scenario where you work for a bakery that needs to secure its system in a FactoryTalk Network Directory:

- You have divided the plant's users into groups named Operators, Shift Leaders, and Supervisors.

You are going to create three new users:

Pat Smith, who will be added to the Shift Leaders user group

Bob Tyler, who will be added to the Operators user group

Leslie Williams, who will be added to the Supervisors user group

- You have divided the bakery into logical areas based on function – Ingredients, Mixing, Baking, and Packaging.

You are going to add the computer group **OpStation1**.

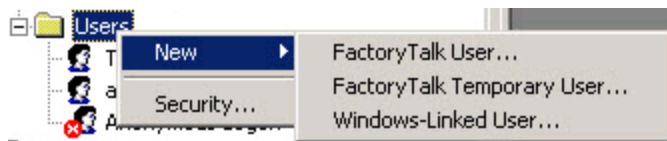
- You have defined system policies for each group.

You are going to set up password policies.

Create a user

The following examples refer to **Computer1** and **Computer2**, which were defined in [Install and activate FactoryTalk software](#) on [page 25](#).

- On Computer1:** In the Explorer window, expand the FactoryTalk Network directory tree, and then expand the **System** folder until the **Users** folder is visible.
- Right-click the **Users** folder, select **New**, and then select **FactoryTalk User**.



- On the **General** tab, type the **User name**, **Full name**, and **Description** and then select the appropriate password options.

Tip: The password options you select here are subject to the policies you select in the Security Policies.

Some FactoryTalk-enabled products can send messages or notifications automatically to an e-mail address. For details, see the documentation supplied with your FactoryTalk-enabled product.

The screenshot shows a Windows-style dialog box titled "New FactoryTalk User". It has two tabs: "General" (selected) and "Group Membership". Under the "General" tab, there are several text input fields: "User name:" containing "PSmith", "Full name:" containing "Pat Smith", "Description:" containing "Shift Leader", and "E-mail:" which is empty. Below these fields are four checkboxes: "User must change password at next logon" (checked), "User cannot change password" (unchecked), "Password never expires" (unchecked), and "Account is disabled" (unchecked). At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help". There are also password fields labeled "Password:" and "Confirm:" with masked characters (dots).

For this example, enter the following:

User name: **PSmith**

Full name: **Pat Smith**

Description: **Shift Leader**

Password: **password**

For this example, clear the **User must change password at next logon** check box, and then select the **Password never expires** check box.

4. Click **OK**. The new user appears in the Users folder.



5. Create two new users for the following:

User name: **BTylerh**

Full name: **Bob Tyler**

Description: **Operator**

Password: **password**

User name: **LWilliams**

Full name: **Leslie Williams**

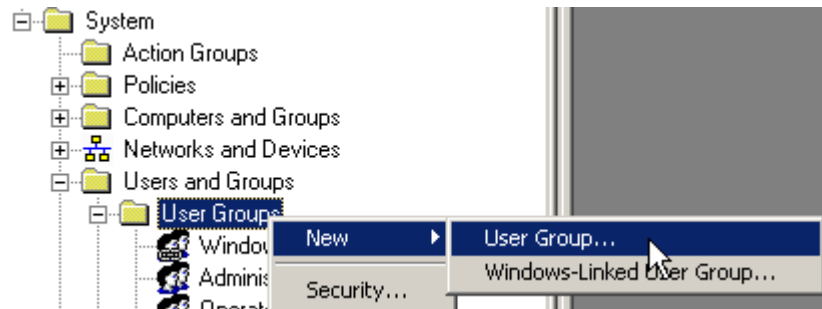
Description: **Supervisor**

Password: **password**

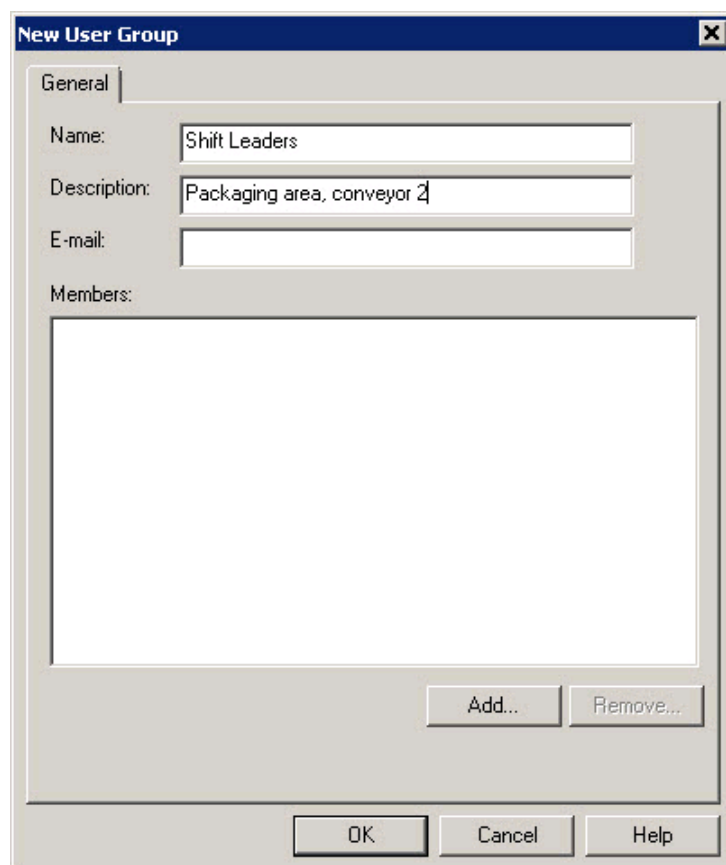
For both users, clear the **User must change password at next logon** check box, and then select **Password never expires**.

Create a user group

1. Right-click the **User Groups** folder, select **New**, and then select **User Group**.



2. Type a **Name** and **Descriptor** (for this example use the information shown below).

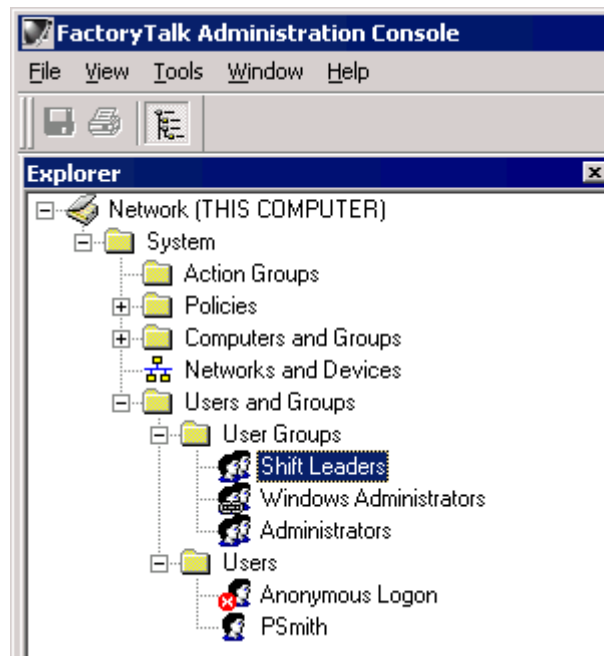


3. Click **Add** to open the **Select User or Group** dialog box. If the user PSmith is not listed, select the **Show All** or **Show users only** check box.



4. Select **PSmith**, and then click **OK** to add PSmith to the Shift Leaders user group.
5. Click **Create** to create the Shift Leaders user group and close the dialog box.

The new group appears in the User Groups folder.



6. Create user groups for Operators (add BTyler) and Supervisors (add LWilliams).

Deleting user accounts

1. In FactoryTalk Administration Console or FactoryTalk View Studio, in the Explorer window, expand the FactoryTalk Network or Local Directory tree, and then expand the System folder until the user account you want to delete is visible.
2. Right-click the user account, and then click **Delete** on the context menu.

All user accounts are identified by means of a unique identifier that is separate from the user name. When you delete a FactoryTalk user account that has been assigned to a FactoryTalk View application, the user's access rights to that application are deleted, but the user account's unique identifier is not. This means that even if you create a user account with the identical name, the new user account will not automatically have access to the same resources that the old one did.

Any applications the deleted user was added to will display the user account's unique identifier instead of the user name (which no longer exists). This unique identifier must also be deleted.

Users	Computers
 Administrators	 All Computers
 All Users	 All Computers
 9C1AEABA_F29E_48F7_82E8_3CDA	 All Computers
 Anonymous Logon	 All Computers

When you create another user account with the same name, you must recreate the security settings of the account. Refer to the "Recreating deleted accounts" section of "Delete a user account" topic in FactoryTalk Help for instructions.

Where to go from here

Do one of the following:

- Continue adding users, groups, and/or computers, if desired.
- Go to [Assigning permission](#) on [page 79](#) to learn about assigning permissions to the users, groups, and computers added in this chapter.
- Go to [Setting up system-wide policies and product policies](#) on [page 93](#) to learn about setting system-wide and policy-wide security policies.
- Go to [Resource grouping](#) on [page 103](#) to learn about FactoryTalk Security advanced features, such as resource grouping and tightening security.
- Go to [RSLink and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLink software.
- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure projects and devices like Logix5000, PLC, and SLC controllers.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components
- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.

Assigning permissions

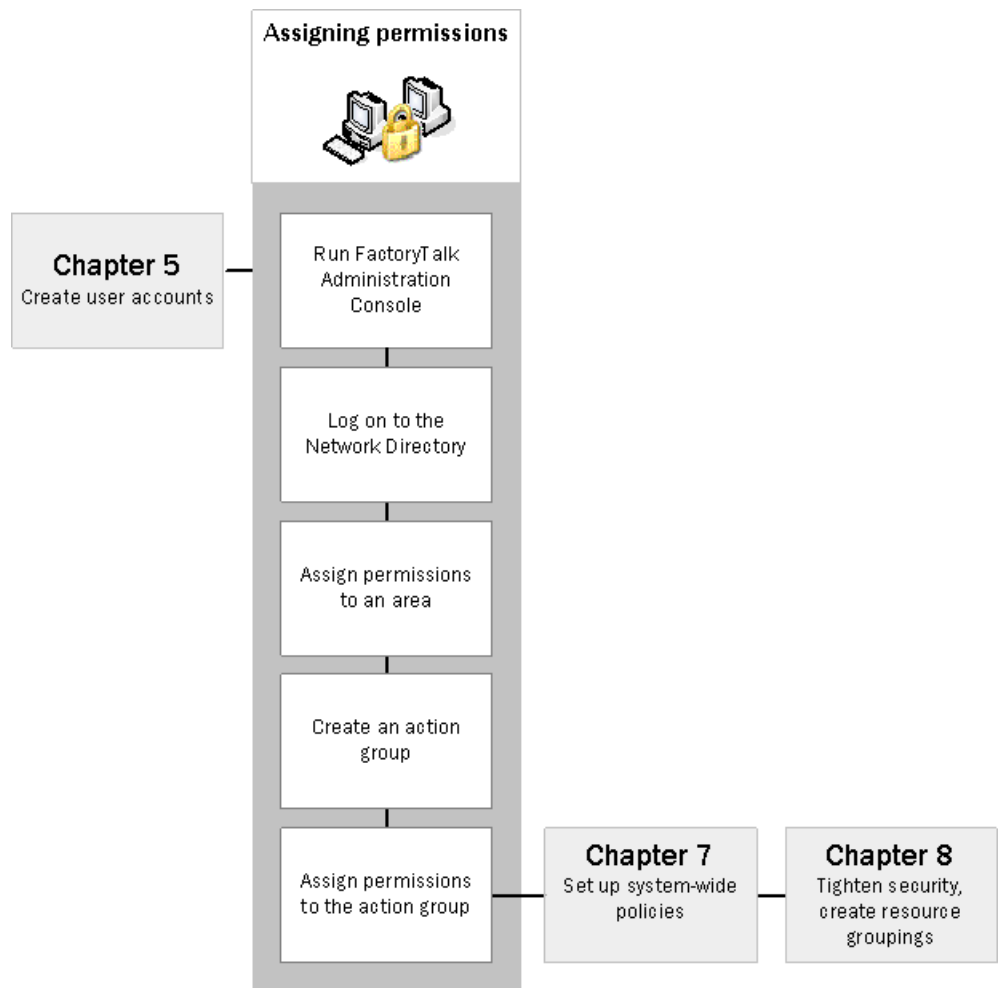
This chapter describes how to assign permission (security rights), including information on:

- allow and deny permissions
- understanding inheritance, and the order of precedence
- categories of permissions
- effective permissions
- action groups
- Verify that you have installed and activated the software listed below under [What you need](#) on [page 79](#).
- Verify that you have configured the Network Directory as discussed in [Specify the Network Directory location](#) on [page 45](#).
- Added user and group accounts as discussed in [Creating user accounts](#) on [page 67](#).
- Become familiar with the terms and concepts of FactoryTalk Security. See [Understanding automation security](#) on [page 17](#) and [About the FactoryTalk system](#) on [page 21](#) for more information.
- FactoryTalk Services Platform v. 2.10 (CPR 9) or later. Using the newest available version is recommended.
- FactoryTalk Security (installed with FactoryTalk Service Platform)

Before you begin

What you need

Follow these steps



Allow and deny permissions

For any resource in your application, for example, the application itself, an area, a server, and so on, you can assign one of two permissions (or rights) – Allow or Deny – to any action a user, computer, or group can perform on an object. For example, you can deny write access to a particular server for certain users, user groups, computer, or computer groups.

You can set two kinds of permissions:

Allow permissions allow users to perform actions on resources from all or from only certain computers on a network.

Deny permissions prevent users from performing actions on resources from all computers or from only certain computers on a network.

You can also remove all permissions from an object by clearing both the Allow and Deny check boxes. This allows the object to inherit permissions assigned at a higher level. For example, if an HMI server is located in an area, and you remove all permissions from the HMI server, the HMI server inherits permissions from the area.

If no permissions are assigned to a resource at any level, Deny is implied.

Follow the best practice below:

- Assign permissions to groups rather than to users.
Because it is inefficient to maintain user accounts directly, assign permissions to user accounts only by exception.
- Wherever possible, remove Allow permissions instead of assigning explicit Deny permissions. This makes administration simpler because of the order of precedence of explicit permissions over inherited permissions, and Deny permissions over Allow permissions.
- Use Deny permissions to:
 - exclude a subset of a group that has Allow permissions
 - exclude one special permission when you have already granted full control to a user or group
- Assign permissions at as high a level as possible. This provides the greatest breadth of effect with the least effort. The rights you establish should be adequate for the majority of users. For example, assign security to areas rather than to objects within areas.
- Administrators should use an account with restrictive permissions to perform routine, non-administrative tasks, and use an account with broader permissions only when performing specific administrative tasks.

Understanding "inheritance"

By default, objects inherit permissions automatically from their parent objects. For example, if you assign security to an area in an application, all of the items in the area inherit the security settings of the area, and the area inherits security settings from the application. The top of the hierarchy is the Network Directory or Local Directory.

Networks and devices that are referenced by logical names, rather than by relative paths, inherit permissions differently than other resources.

You can override inherited permissions in two ways:

- **Set up explicit permissions** for resources at a lower level of the hierarchy. For example, if an area inherits permissions from an application, you can override the inherited permissions by specifying permissions explicitly for the area.
Explicit permissions are assigned deliberately to users, groups, or computers for objects or actions. Explicit permissions take precedence over inherited permissions.
- **Break the chain of inheritance** at a level in the Network Directory or Local Directory tree. For example, you can stop an area from inheriting permissions from the application in which it is located. To do this,

select the "Do not inherit permissions" check box when setting up security for the resource. When you break the chain of inheritance, you can specify whether to remove all permissions from resources below the break (which implies Deny permission), or whether to use the permissions that are inherited by the resource at the break as explicit permissions.

Permissions can be inherited only as far up the Network Directory or Local Directory tree as the chain of inheritance remains intact. For example, if you select the "Do not inherit permissions" check box for an area, items that inherit permissions inside the area can inherit permissions only as far as the area. They cannot inherit permissions from the application in which the area is located. Because breaking the chain of inheritance complicates administration, you should do so only when absolutely necessary.

The principle of inheritance allows you to set permissions at as high a level as is practical, and then introduce exceptions at lower levels where necessary.

If permissions are not assigned at any level, Deny is implied.

When the system evaluates the level of access a user, computer, or group has, the following rules apply:

Order of precedence

- **Deny permissions are implied.** If you do not assign any permissions to a resource, Deny is implied. Use implied Deny permissions rather than explicit Deny permissions wherever possible, because this simplifies administration.
- **Deny permissions are evaluated before Allow permissions.** For example, if the Operators group is denied access to a data server, but an individual user account (Jane) is granted access to the data server, Deny takes precedence over Allow, and Jane cannot access the data server because she is a member of the Operators group.
- **Explicit permissions override inherited permissions.** For example, assume your application has an area called Baking, and you allow Operators to have Read access to the area. If you deny operators Read access to an HMI server in the Baking area, the Deny permission takes precedence over the Allow permission.

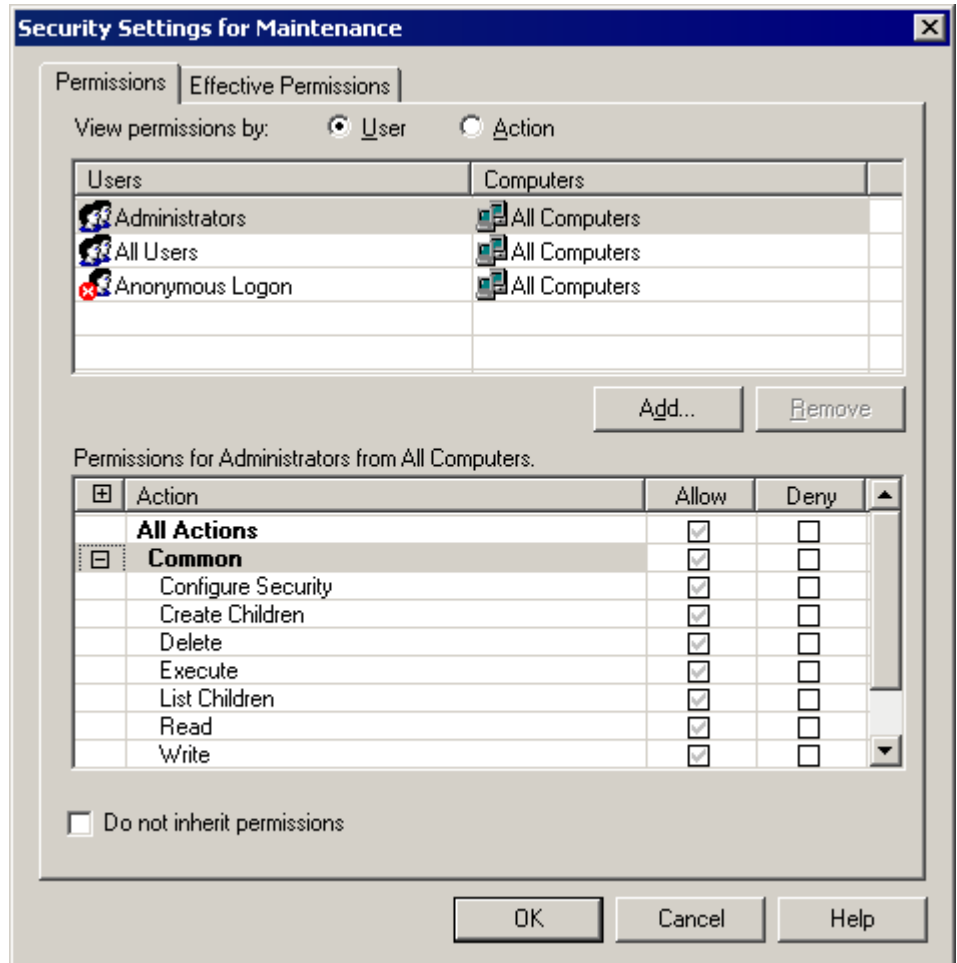
This means that an explicit Allow permission overrides an inherited Deny permission, and an explicit Deny permission overrides an inherited Allow permission.

- **If conflicting explicit permissions are set at the same level, Deny takes precedence over Allow.** For example, if you explicitly deny the Operators group access to a data server, but you explicitly allow an individual user account (Jane) access to the data server, Deny takes precedence over Allow, and Jane cannot access the data server because she is a member of the Operators group. This happens because conflicting explicit permissions are set on the same resource. To Allow Jane access to the data server, you must Deny the Operators group

Categories of permissions for actions

access to a resource at a higher level in the hierarchy (for example, the area in which the data server is located), and then explicitly allow permissions for the data server.

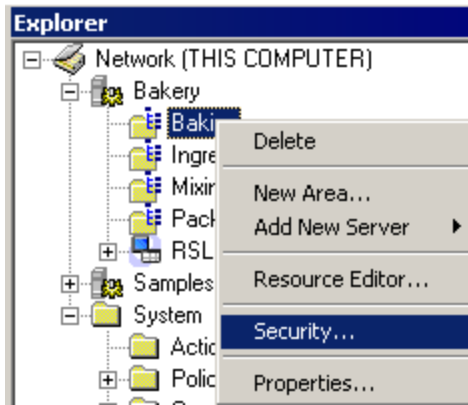
The actions that users can perform on resources are grouped into categories. The Common category is common to all FactoryTalk products. For details about the actions in the Common category, see FactoryTalk Security online help.



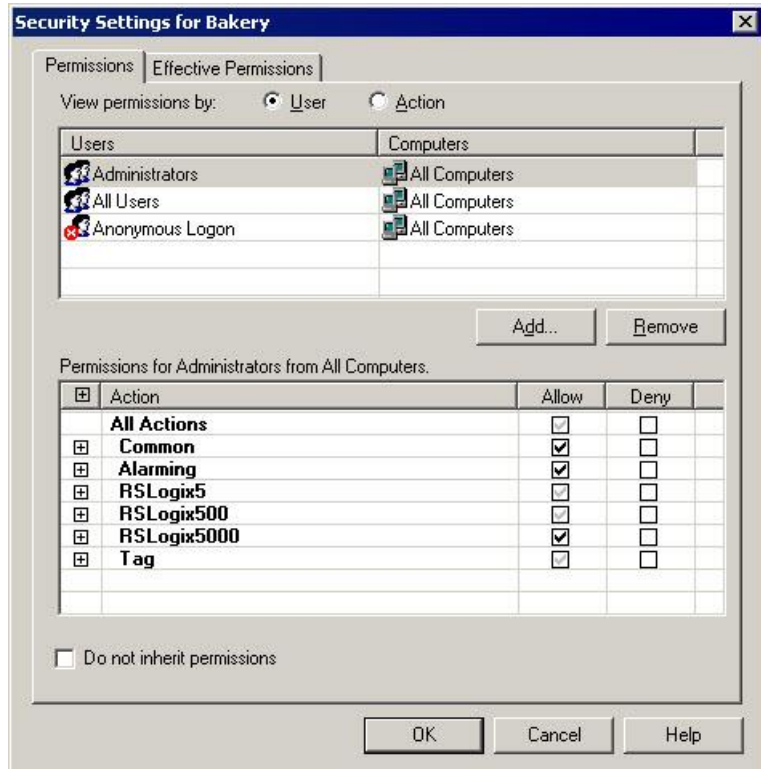
You can create your own groupings for actions. This allows you to assign security permissions to all of the actions in the group in one step rather than assigning permissions to each action separately. See [Creating action groups](#) on [page 87](#) later in this chapter.

Assigning permissions

1. In FactoryTalk Administration Console, right-click the directory object, for example, the application, area, or server, for which you want to define security, and then click **Security** on the pop-up menu. For this example, select **Baking**.



2. In the **Security Settings** dialog box, click the **Permissions** tab.
3. In the list of users and computers, click **Add**, and then select the combination of users, computers, and groups for which you want to define permissions.



In the list of permissions, select the check boxes that correspond to the actions you want to allow or deny. To allow security to be inherited from a

higher level, clear both Allow and Deny check boxes. When you are finished, click **OK**.

The check boxes indicate what permissions will be in effect when you click **OK**:

☐ A blank check box beside an action means that no permissions are assigned. If both the Allow and Deny check boxes are cleared beside an action, Deny is implied for the action.

However, a blank check box shown beside the name of a group of actions, for example, All Actions or Common, means that some of the actions within that group do not have permissions assigned. If collapsed, you must expand the group to see which actions do not have permissions assigned.

☒ A black check mark means that Allow or Deny permissions have been assigned explicitly.

☐ A gray check mark means that Allow or Deny permissions have been inherited.

Tip: Wherever possible, remove Allow permissions instead of assigning explicit Deny permissions. This makes administration simpler because of the order of precedence of explicit permissions over inherited permissions, and Deny permissions over Allow permissions.

Viewing permissions

You can view the security you've set up for resources. Permissions are shown for:

- a user or group of users
- a computer or group of computers

For example, when you view effective permissions for an application, the **Effective Permissions** tab can show whether the selected users and computers can read the contents of the application.

To view the permissions in effect for a computer or group of computers, you must be using a FactoryTalk Network Directory. You cannot view effective permissions for computers or groups of computers in a FactoryTalk Local Directory, because a FactoryTalk Local Directory is restricted to a single computer.

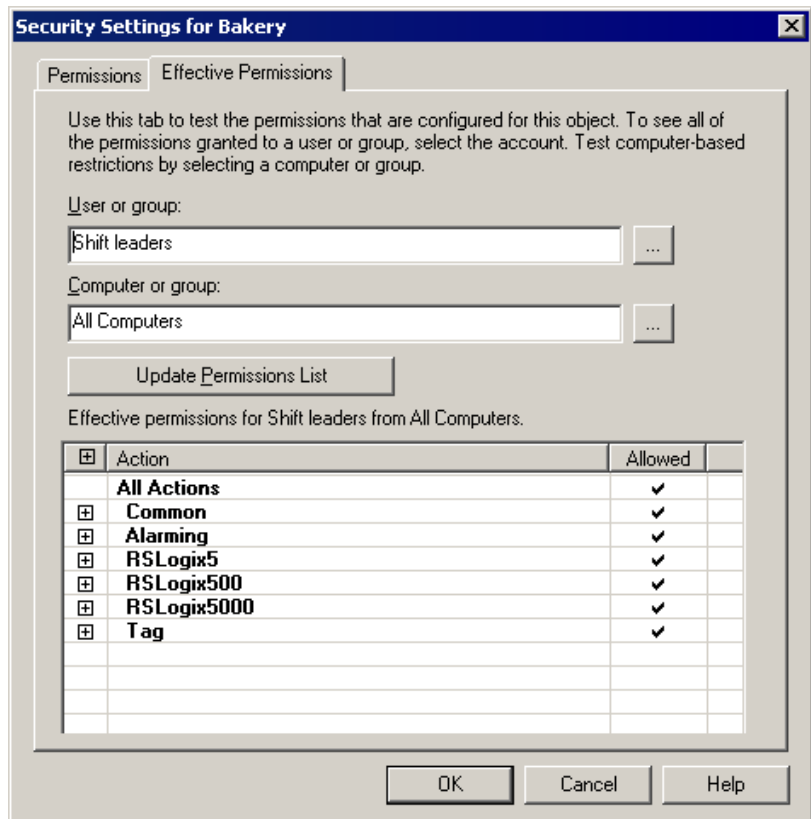
Understanding effective permissions

The **Effective Permissions** tab does not show separate columns for Allow and Deny permissions, and does not distinguish between explicit and inherited permissions. Instead, the presence or absence of a check mark in the Allowed column indicates the permissions in effect on the directory object for the selected user and computer, or group:

- If a check mark appears beside an action, the action is allowed, whether explicitly or by inheritance.
- If a check mark does not appear beside an action, the action is denied, whether explicitly or by inheritance.
- If an action category (for example, Common or Alarming) shows a gray check mark, one or more – but not all – of the actions inside the category are allowed. Expand the category to see which actions are allowed or denied.

To view effective permissions:

1. In the Explorer window of the FactoryTalk Administration Console, expand the FactoryTalk Directory tree, and then expand the **System** folder until the resource for which you want to view effective permissions is visible. For example, to view effective permissions for an application, expand the tree until the application is visible.
2. Right-click the resource, and then click **Security** on the pop-up menu.
3. Click the **Effective Permissions** tab.



4. In the **User or group** box, type the name of a user or group of users, or click the Browse button to browse for a user or group.

5. In the **Computer or group** box, type the name of a computer or group of computers, or click the Browse button to browse for a computer or group.
6. Click **Update Permissions List**.

The Effective Permissions list shows the permissions currently in effect for the selected users and computers.

Creating action groups

Action groups allow you to group actions together and then assign security permissions to all of the actions in the group. This allows you to grant or deny permissions for a set of actions in one step, rather than having to set permissions for each action separately.

Create action groups that make sense in your facility. For example, create groups based on:

- a person's role or job (operator, supervisor, engineer, and so on)
- the equipment a person has access to (hoppers, mixers, ovens, and so on)

Available *Common* actions are Configure Security, Create Children, Delete, Execute, List Children, Read, and Write. Available *product-specific* actions depend on the product installed. The available actions for FactoryTalk Alarms and Events, for example, are Acknowledge, Enable/Disable, Reset, and Suppress.

Use action groups to assign permissions for a set of actions in one step rather than having to set permissions for each action separately. When adding an action group, you decide:

- the name of the action group
- what actions belong to that group

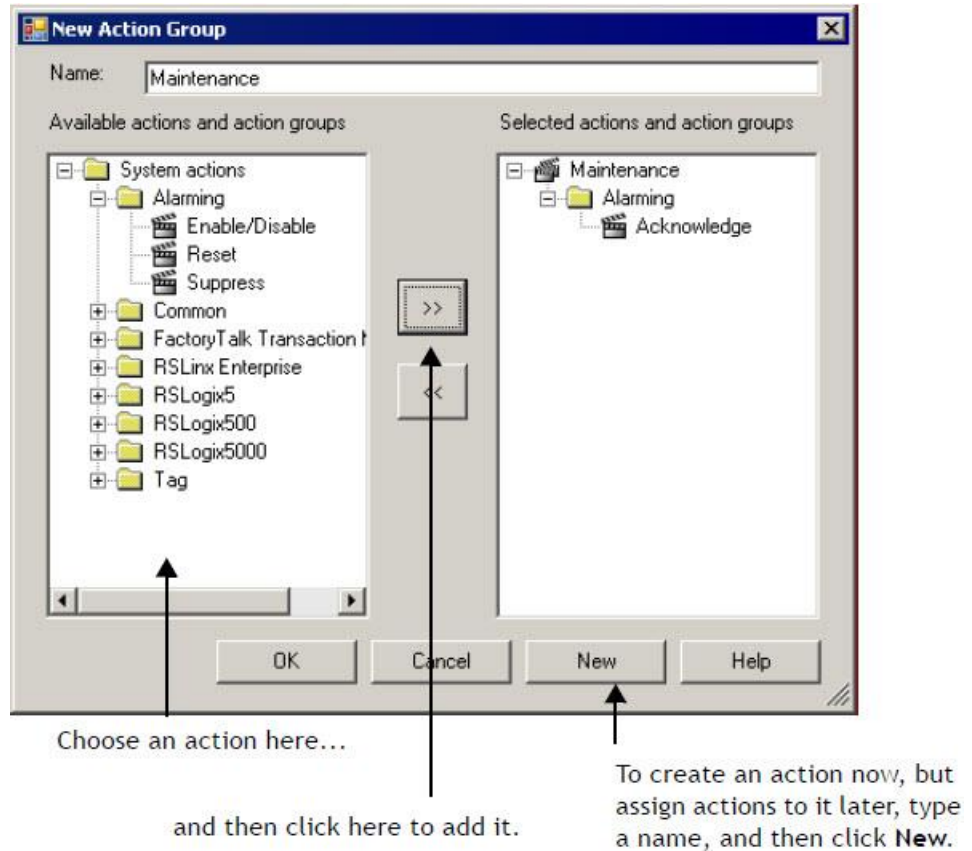
Create the action groups for our example scenario

1. In the FactoryTalk Administration Console, click the **Systems** folder, right-click the **Action Groups** folder, and then select **Add New Action Group** from the pop-up menu.



Tip: You will be notified that using Action Groups with mixed versions of FactoryTalk Services Platform may cause undesired results. If you have installed FactoryTalk Services Platform for the first time, and have no versions of FactoryTalk Automation Platform installed, click **Yes** to continue.

2. Type a unique name for the action group (for this example use **Maintenance**), select the allowable actions for the action groups, and then click **OK**.



This name will appear in the **Security Settings** dialog box, under the User Action Groups category.

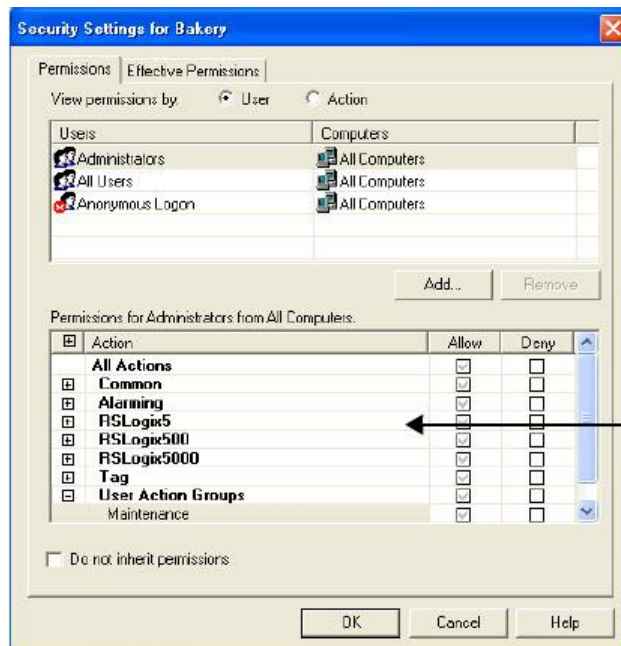
Assign action group to an application

1. Right-click the name of the application, and then click **Security** on the pop-up menu.



2. Select the Maintenance action group, assign the appropriate permissions, and then click **OK**.

Assigning Allow or Deny permissions to the action group, automatically assigns the permissions to the individual actions within the group.



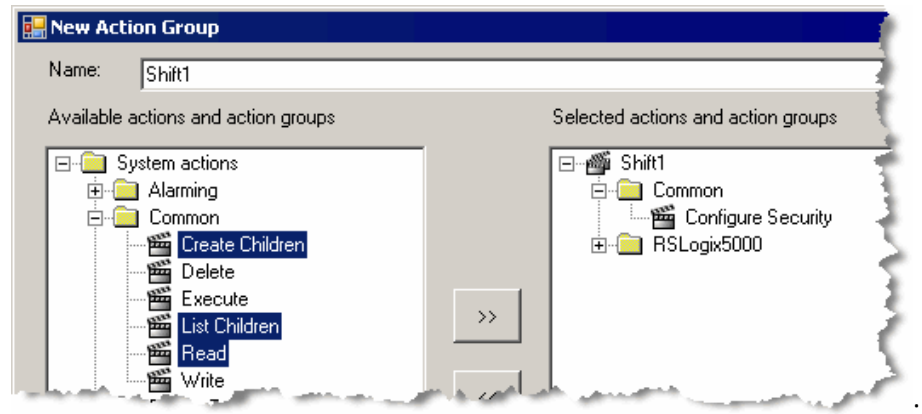
These categories are always here.

Working with action groups

Following are some tips for working with action groups.

Creating new action groups

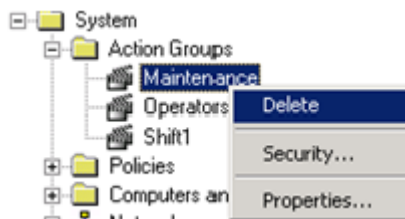
When you create a new action group, you can move items one by one, or do the following:



- Select the folder
- Use shift-click to select multiple consecutive items
- Use ctrl-click to select multiple non-consecutive items

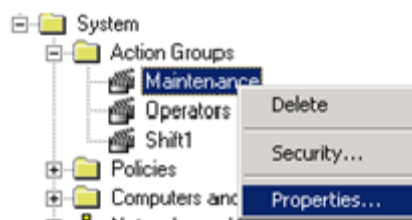
Deleting action groups

To delete an action group, right-click it, and then select **Delete** from the pop-up menu.



Editing action groups

To edit an action group, right-click it, and then select **Properties** from the pop-up menu.



Renaming action groups

You cannot rename an action group. Instead, make a note of the permissions assigned to the action group you want to rename, delete the action group, and then add the new action group. Recreate the permissions for the new action group.

You cannot nest action groups

To prevent conflicting permissions, you cannot include (nest) action groups within other action groups.

Beware of conflicting permissions when including the same action in multiple action groups

You can include the same action in multiple action groups, however this can cause conflicting permissions. For example, if the same action is included in two groups that apply to the same resource, and you explicitly Allow permission for the first action group, ut explicitly Deny permission for the second action group, the user will be denied permission for the action that the two action groups have in common because Deny permissions always take precedence over Allow permissions.

Where to go from here

Do one of the following:

- Continue adding action groups and assigning permissions, if desired.
- Go to [Setting up system-wide policies and product policies](#) on [page 93](#) to learn about setting system-wide and policy-wide security policies.
- Go to [Resource grouping](#) on [page 103](#) to learn about FactoryTalk Security advanced features, such as resource grouping and tightening security.
- Go to [RSLinx and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLinx software.
- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure project, and securing devices like Logix5000, PLC, and SLC controllers.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components
- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.

Setting up system-wide policies and product policies

This section describes how to set up:

- system-wide policies
- product policies

A policy is a setting that applies across the entire FactoryTalk manufacturing system. For example, all FactoryTalk products that share a single FactoryTalk Directory use the same audit policy setting that records a user's failure to access a secured object or feature because the user has insufficient security permissions. If you disable this policy, none of the FactoryTalk products in your system will record failed attempts to access secured objects or features.

System policies

Some examples of FactoryTalk system-wide policies include:

- **Security policies**—minimum password length, complexity requirements, password expiration requirements, and so on. These policies do not apply to Windows-linked accounts. Define policies for Windows-linked accounts in Windows.
- **Audit policies**—whether access checks are audited, whether access grants, denies, or both are audited, and so on.
- **User rights assignment policies**—whether users can back up and restore the contents of FactoryTalk Directory, change the directory server, switch between primary and secondary servers in redundant pairs, or modify the security authority identifier.

See [System-wide policies](#) on [page 95](#) for more information.

Product policies

A product policy secures either a system-wide feature or system-wide configuration data that is specific to a particular product. Each FactoryTalk product provides its own set of product-specific policies, which means that the product policies available on your system vary, depending on which FactoryTalk products you have installed. See [Product policies for more information](#) on [page 98](#).

For specific details about setting up policies for installed products, see Help for each product.

Important: Product policies **do not** inherit security settings. When specifying permissions for product policies, clearing both the Allow and Deny check boxes does not allow the policy setting to inherit security. Instead, clearing both check boxes **denies access** to the product feature.

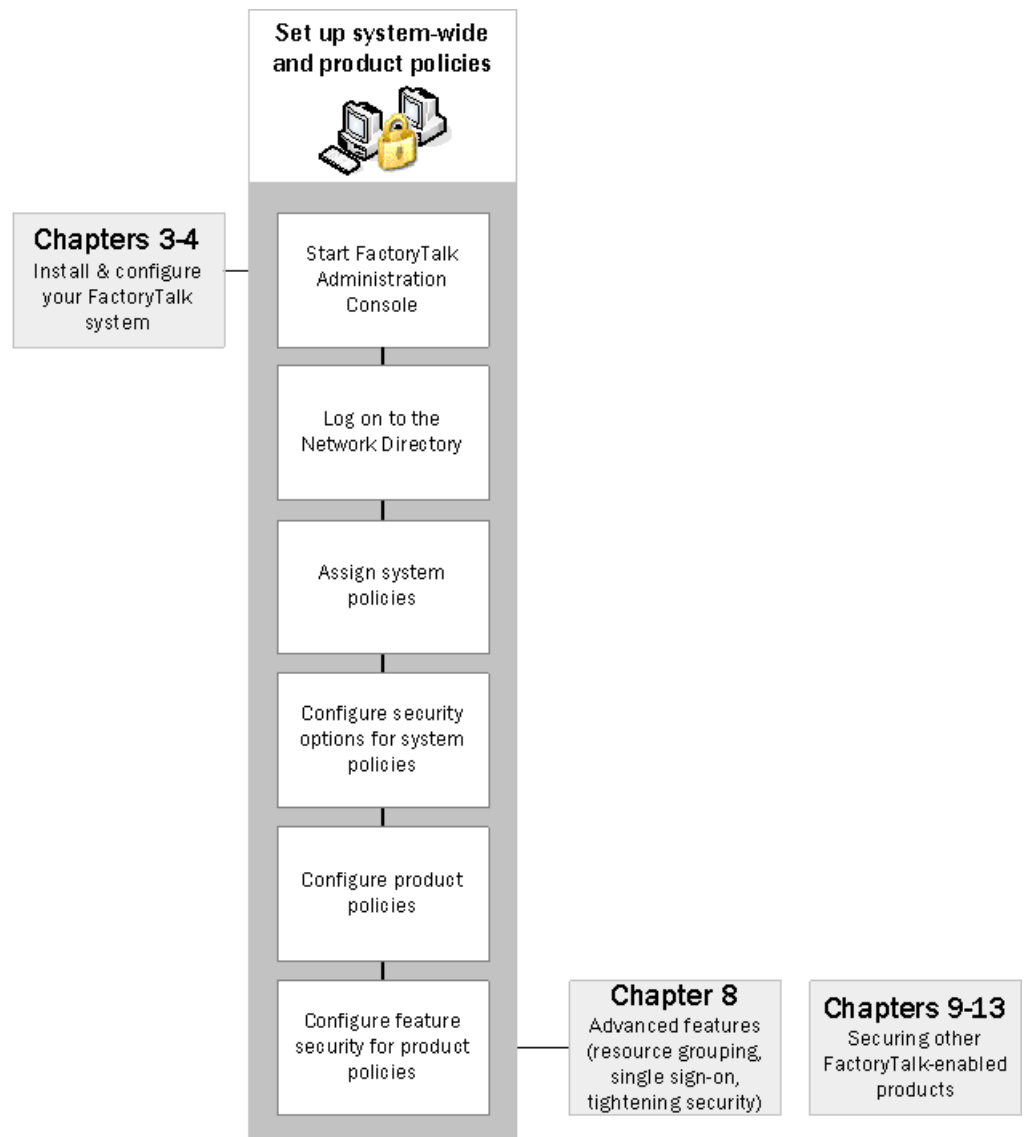
Before you begin

- Verify that you have installed and activated the software listed below under [What you need](#) on [page 94](#).
- Verify that you have configured the Network Directory as discussed in [Specify the Network Directory location](#) on [page 45](#).
- Become familiar with the terms and concepts of FactoryTalk Security. See [Understanding automation security](#) on [page 17](#) and [About the FactoryTalk system](#) on [page 21](#) for more information.

What you need

- FactoryTalk Services Platform v. 2.10 (CPR 9) or later. Using the newest available version is recommended.
- FactoryTalk Security (installed with FactoryTalk Service Platform)

Follow these steps



System-wide policies are security settings that apply across the entire FactoryTalk automation system. They include:

- FactoryTalk Alarms and Events policies, which determine the system-wide behavior of alarms and events
- Application authorization policies allow you to authorize applications that have access to FactoryTalk Directory and to configure whether to verify the application publisher information.

Important: Some applications of Microsoft (for example, msixec.exe) are not signed. Some earlier versions of FactoryTalk products were not signed when they were released. You may fail to verify the publisher information on these applications. For more information about versions of FactoryTalk products signed, see FactoryTalk Security Help.

- User rights assignment policies allow you to secure features in FactoryTalk Directory, and to specify what **FactoryTalk** users and

groups can access those features. For example, you can specify which users are allowed to back up and restore your FactoryTalk system.

Important: Assigning user security policies within FactoryTalk Directory applies only to FactoryTalk users and groups. It does not affect Windows users and groups outside of FactoryTalk. For example, if the minimum password length for FactoryTalk native users is set to 5 characters, and the user has a Windows-linked account with a Windows policy of 6 characters, the Windows policy will be enforced by Windows.

- Live Data Policy allows you to configure system-wide settings related to data.



Changing health monitoring policy settings can result in unexpected behavior. For most networks, the default policy settings provide the best results.

- Health Monitoring Policy allows you to fine-tune the parameters that the health monitoring service uses when determining whether a network glitch is occurring and how long to wait before switching to a Standby server.



Changing live data policy settings can result in unexpected behavior. Do not change the settings in a running production system. For changes to take effect, all computers on the network must be shut down and restarted.

- Audit policy determines what security-related information is recorded (audited) while the system is being used. For example, you can track when users are denied access to resources in your system.
- Security policy defines general rules for implementing security across all FactoryTalk products in your system. For example, you can control the number of times a user can attempt to log on unsuccessfully before the user's account is locked.

Tip: Another policy setting is Single Sign-on, which determines whether users can log on once to the FactoryTalk system or must log on to each FactoryTalk product separately.

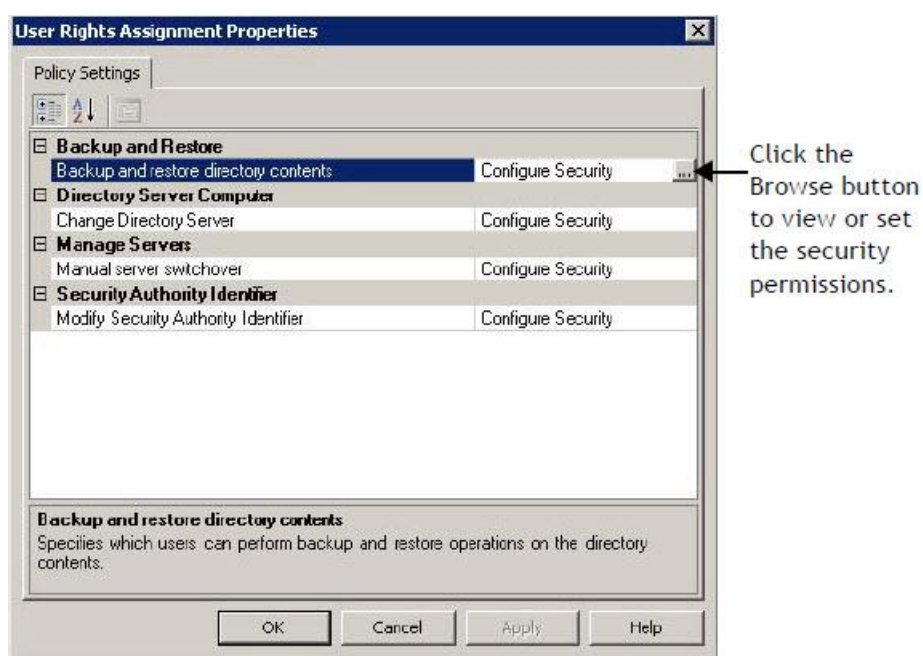
Assigning system policies

1. Start FactoryTalk Administration Console and log on to the FactoryTalk Directory where you want to configure product policies. For this example, log on to the Network Directory.
2. In the Explorer window, expand the Network or Local FactoryTalk Directory tree, and then expand the folders **System** > **Policies**

3. Right-click a policy, and then select **Properties** from the pop-up menu.



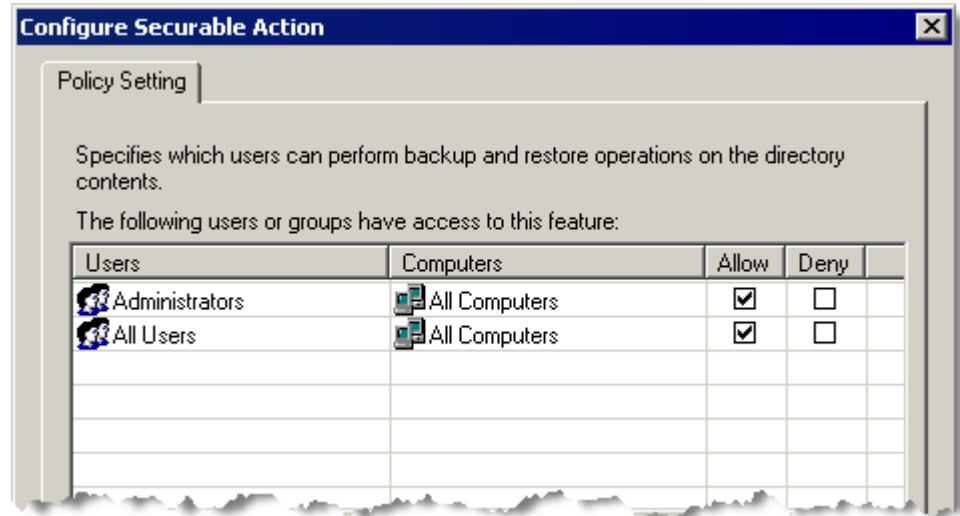
4. Select the policy for which you want to assign security.



5. Configure the security options.

The security options for each product are different – in some cases, you are simply enabling or disabling something. In other cases, you are assigning time limits and other types of parameters.

In the User Rights Assignment Properties dialog box shown above, clicking the browse button opens the dialog box for assigning user/user groups the specific right.



6. Click **OK** to save the policy settings.

Product policies

Product policies are security settings that restrict access to the features of individual FactoryTalk products in your system to prevent inadvertent changes or tampering. Only users with the required level of access can use the product features you have secured.

For example, when you set up product policies for RSLinx Classic, you might restrict the ability to shut down the RSLinx Classic service to a small group of users, to prevent parts of your automation system from going down at runtime.

Each FactoryTalk product you install provides different securable features.

In the case of a FactoryTalk Local Directory, a product policy applies to the product installed on the computer where the Local Directory is located.

In the case of a FactoryTalk Network Directory, a product policy applies to all installations of the FactoryTalk product on all computers that are connected to the FactoryTalk Network Directory.

Product policies and inheritance

- Product policies inherit their security settings from a special item, called Feature Group Security. The Feature Group Security item might be available or unavailable in the list of securable features in the **Feature Security Properties** dialog box, depending on what FactoryTalk products you have installed.
- If the Feature Group Security feature is available and you remove both Allow and Deny permissions for a feature, the user is denied access to the feature.

Important: Product policies **do not** inherit security settings. When specifying permissions for product policies, clearing both the Allow and Deny check boxes does not allow the policy setting to inherit security. Instead, clearing both check boxes **denies access** to the product feature.

For example, in the case of RSLinx Classic, this means that product policies for RSLinx Classic do not inherit their security settings from the RSLinx Classic folder in which they are located.

How are product policies and actions different?

A securable action applies to all products that use that action in a particular context (the context being whatever resource you are securing the action for example, a FactoryTalk Directory, application or area).

A product policy applies to only one product – if you are denied permission to a product feature, you cannot use that product feature when using that product in any context.

In some cases, there are securable actions and product policies for the same capability. For example, Logix Designer application has both a securable action and a product policy called **Firmware: Update**.

- The securable action applies to all products – if you are denied permission to the Firmware: Update action in an application or area, you cannot update firmware in the controller from that application or area using any product.
- The product policy applies to only Logix Designer application – if you are denied permission to Firmware: Update, you cannot update firmware when using Logix Designer to configure any controller.

Unlike securable actions for resources, product policies do not inherit security settings. When specifying permissions for product policies, clearing both the Allow and Deny check boxes does not allow the policy setting to inherit security. Instead, clearing both check boxes denies access to the product feature, and causes the user/computer entry to be removed from the product policy configure securable action dialog box..

Two different ways to configure feature security

Typically you will want to configure security for multiple products and features at once. Use the **Feature Security for Product Policies** dialog box to do this.

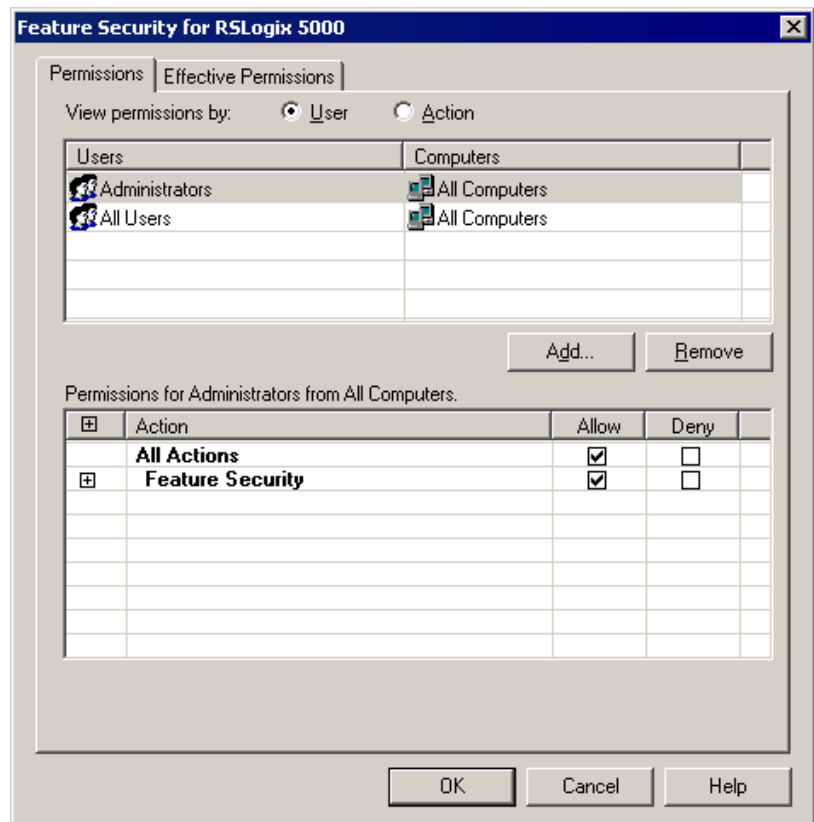
Configure multiple products

1. Start FactoryTalk Administration Console or FactoryTalk View Studio and then log on to the FactoryTalk Directory where you want to configure product policies.

2. In the Explorer window, expand the Network or Local FactoryTalk Directory tree, and then expand the folders **System** > **Policies**.
3. Right-click **Product Policies**, and then select **Configure Feature Security** from the pop-up menu.

You can also right-click any of the individual product categories and then click Configure Feature Security to configure policies for just that product.

4. In the **Feature Security** dialog box, assign the appropriate security permissions, click the plus (+) sign next to the Feature Security text to see all of the permissions for the product, and then click **OK**.



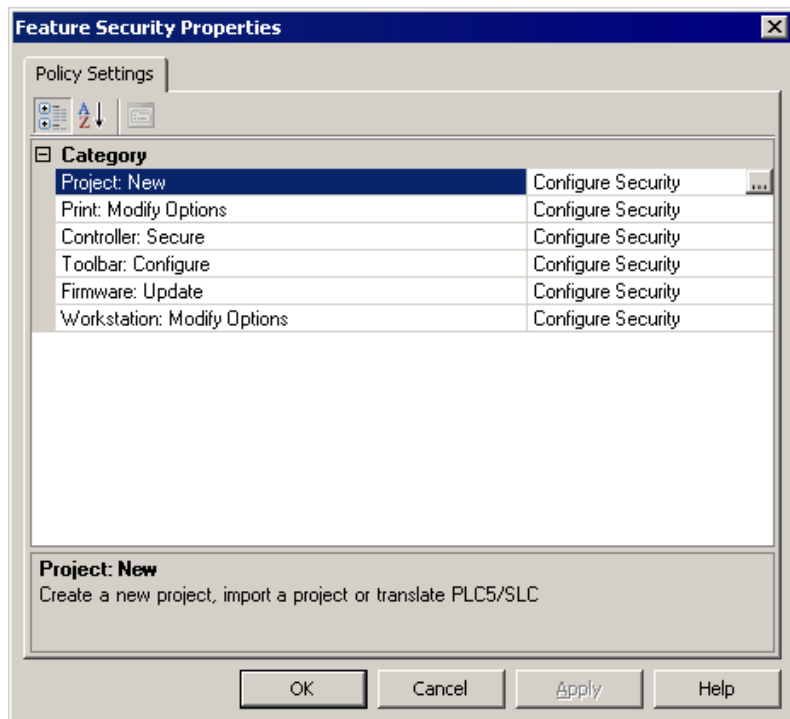
Configuring a single product feature

1. In the Explorer window, expand the Network or Local FactoryTalk Directory tree, and then expand the folders **System** > **Policies** > **Product Policies**.

- In the Product Policies folder, expand the folder for the product whose features you want to secure and then double-click **Feature Security** or the name of the feature you want to secure.



- In the **Feature Security Properties** dialog box, click the row containing the feature you want to secure. A description of the feature appears at the bottom of the **Feature Security Properties** dialog box.



- Configure the security settings for the feature by clicking the browse button (shown at left), and then clicking **OK**.

Important: Please note that FactoryTalk Batch has product policies that can only be configured from the Feature Security folder — they are not available from the pop-up menu. Refer to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) for more information.

Where to go from here

Do one of the following:

- Continue setting up policies, if desired.
- Go to [Resource grouping](#) on [page 103](#) to learn about FactoryTalk Security advanced features, such as resource grouping.
- Go to [RSLinx and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLinx software.
- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure projects.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components
- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.

Resource grouping

This section introduces an advanced security feature called *resource grouping*. Resource grouping is an alternative way to apply security to your hardware resources. Rather than assigning security individually to each resource in the Networks and Devices tree, you group related hardware into an application or area, and then apply security to them. This allows you to assign the same permissions to hardware resources in one step rather than assigning them separately for each resource.

Applying security this way obviously saves time – when you’ve got hundreds of resources that require security, it’s quicker to group them than to do them one by one.

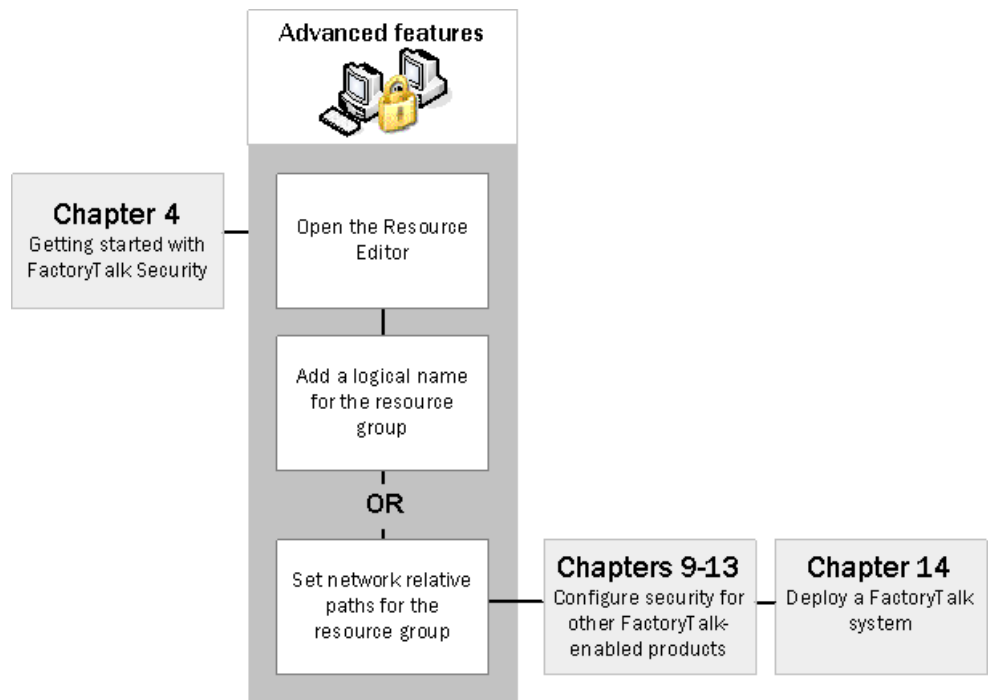
Before you begin

- Verify that you have installed and activated the software listed below under [What you need](#) on [page 103](#).
- Become familiar with the terms and concepts of FactoryTalk Security. See [Understanding automation security](#) on [page 17](#) for more information.

What you need

- FactoryTalk Services Platform installed with a Network Directory configuration. Using the newest available version is recommended.
- An application called **Bakery** created in the Network Directory. See FactoryTalk Help for instructions on creating an application.

Follow these steps



Using resource groupings

Resource groupings allow you to group together control hardware represented in the Networks and Devices tree, and then configure security for the grouping in one step.

Tip: You must have a configured application in order to use resource grouping.

You can group actions together and then assign security permissions to all of the actions in the group. See "About action groups" in FactoryTalk Help.

Why is it called resource "grouping"?

Throughout FactoryTalk Security, there is the concept of creating "groups", such as, user groups and action groups. In these cases, you create a group, name that group, and then assign permissions to the accounts or actions in those groups.

Resource grouping doesn't work that way. In this case, you are taking hardware resources and grouping them into a particular application or area. The resource grouping inherits the rights of that application or area.

Resource grouping and the Networks and Devices tree

Think of resource grouping as the "logical" representation of your plant, and the Networks and Devices tree as the "physical" representation of your plant.

The logical representation allows you to group resources within an application or area – in whatever manner suits your needs – regardless of their physical location.

The Networks and Devices tree, on the other hand, allows you to work with the resources in their physical location on the network.

For example, Norm's Bakery has three separate fans running in three separate areas of the bakery. The Maintenance department is in charge of all the fans, regardless of their location, and controls when they are on and off. To set up security, the system configurator grouped the controllers for the fans in the area called Maintenance, and then assigned security permissions to the area. All the controllers in that area inherited the same security permissions.

How networks and devices inherit security permissions

The security system applies inherited security permissions differently, depending on whether control hardware, available to a local computer through RSLinx Classic, is secured by a network relative path or a logical name, and depending on whether the device is a member of a resource grouping.

A resource grouping allows the network or device to inherit its permissions from the application or area that the resource grouping is associated with, instead of inheriting its security permissions from the System folder, the Networks and Devices node, and then the items within the Networks and Devices folder, down to the device itself.

This means that resource groupings allow networks and devices to inherit their security permissions just like any other resources located inside an application or area, simplifying administration. For details about inheritance, see "About permissions" in FactoryTalk Help.

If the network or device is a member of a resource grouping, and is also associated with a logical name, the device inherits its security permissions from the logical name and *then* from the application or area the resource group is associated with.

How inheritance applies to network relative paths

Control networks and devices that are referenced by network relative paths inherit security permissions in the same way as any other securable resource. Security permissions are inherited from the resource and then up through the entire path to the Network Directory or Local Directory at the top of the Explorer window.

This means that control devices that are accessible through multiple paths can have multiple sets of security permissions. For more information about inheritance and permissions, see "About permissions" in FactoryTalk Help.

How inheritance applies to logical names

Control networks and devices that are referenced by logical names inherit security permissions from only the logical name itself, then the top of the Networks and Devices tree, then the System folder, and finally the Network Directory or Local Directory itself.

When referenced by a logical name, a control device does not inherit security permissions from within the Networks and Devices tree.

Planning how to group resources

When grouping networks or devices, you first have to decide:

- which area you want to associate the resource grouping with.
Typically, choose an area that already has the security permissions you want the network or device to inherit.
- what resources belong to that resource grouping

Once you have added a resource grouping to an area, and added devices to the resource grouping, you do not have to do anything further to make security for the resource grouping work. The devices within the resource grouping automatically inherit the security settings of the application or area where the resource grouping is located.

Creating exceptions for individual networks or devices

You can create exceptions for individual networks or devices by specifying security settings for them explicitly. However, you set up these explicit permissions by browsing for the network or device in the Networks and Devices tree, not in the application or area tree.

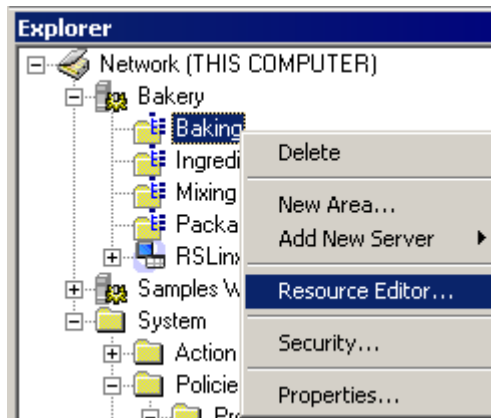
The same device cannot be a member of multiple resource groupings

To prevent conflicting permissions, you cannot include (nest) resource groupings within other resource groupings, and you cannot include the same network or device in multiple resource groupings within the same FactoryTalk Directory.

Instead, you assign permissions to networks and devices at the application and/or area level, so you don't have to assign it individually using the Networks and Devices tree.

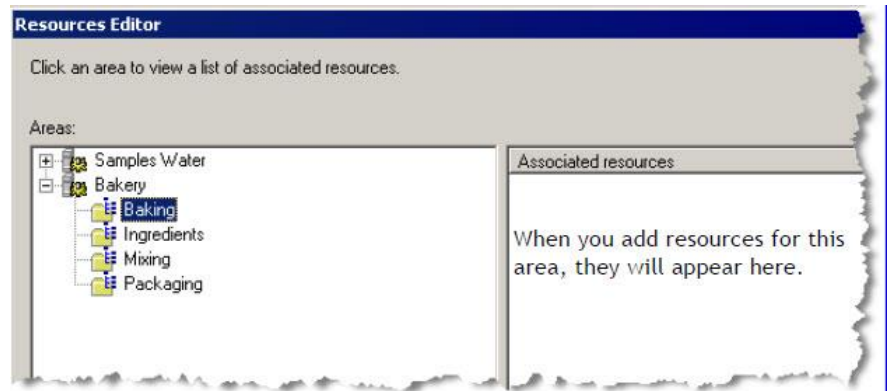
Using the Resource Editor

1. To open the Resource Editor, highlight an application or area, right click, and then select **Resource Editor**.



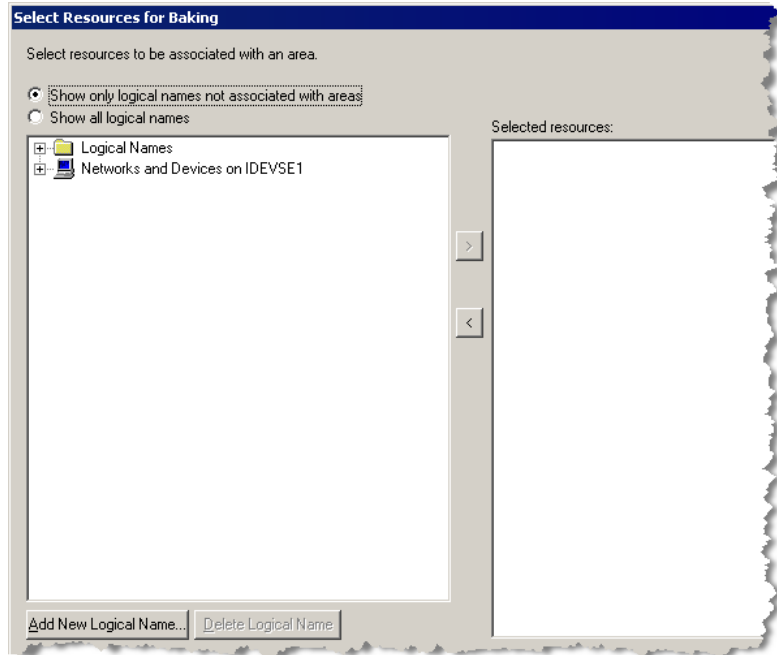
Tip: You will be notified that using resource groups with mixed versions of FactoryTalk Services Platform may cause undesired results. If you have installed FactoryTalk Services Platform for the first time, and have no other versions of FactoryTalk Automation Platform installed, click **Yes** to continue.

The Resource Editor opens.



Add Resources...

2. To add resources, click the **Add Resources** button and then select the resources you want for the application or area.



- If you are using only network relative paths, ignore the options at the top of the dialog box.
 - If you are using logical names, use the options to view all the logical names for the resources in your system, or view only the ones you have not already assigned.
 - Click > to add a resource, and click < to delete a resource.
 - Click **Add New Logical Name** to create a new logical name, so you can add the logical name to an application or area.
 - Click **Delete Logical Name** to delete names that are no longer in use in the system, but are still visible in this window. This can happen if you added a logical name, but later removed the device associated with that name. If the logical name is in use, this button is disabled.
3. When you are done, click **OK** to close the dialog box.

Adding a logical name

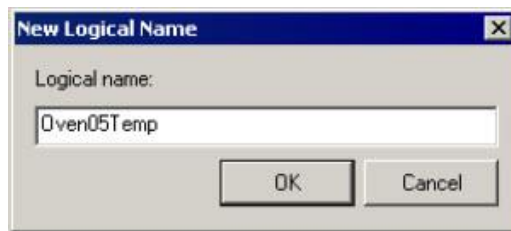
A logical name is an alias that identifies a control network or device. You can use the logical name to provide a shorter or more intuitive name to identify a device instead of using its network relative path. Logical names also change the way devices inherit security permissions.

Why use logical names?

Control devices with identical logical names share security permissions across different control networks and across different computers, without requiring identical RSLinx Classic driver names or relying on identical network paths. For examples of how to use logical names, see Configuration scenarios for networks and devices and How logical names map to network relative paths.

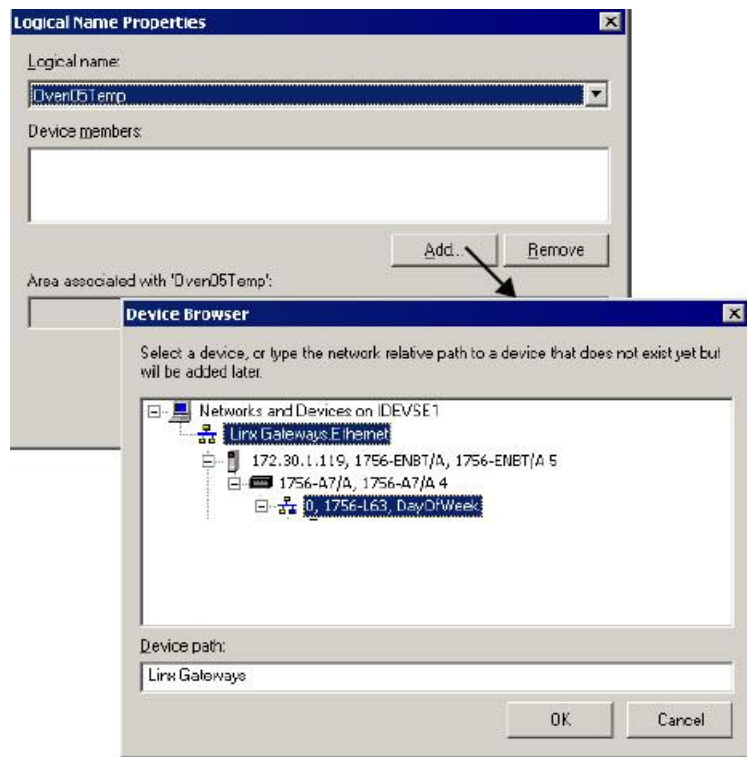
You must define logical names in FactoryTalk Administration Console before configuring security for Logix5000 controllers. For details, see [Enable security for Logix Designer application](#) on [page 126](#). For all other types of control hardware, you can choose whether to associate security settings with logical names or with network relative paths. You might choose to define logical names as aliases for control devices with multiple paths, to associate each instance of the device with a single set of security permissions.

1. To add a logical name, click the **Add New Logical Name** button and enter the logical name you want to use. For this example, use **Oven05Temp**.



The name cannot contain spaces or the \$!:/\? characters

2. Select a resource or type the network relative path to a device. When you're done, click **OK** in both windows to return to the Resource Editor.



Important: Security can be assigned to either the logical name or the relative path, depending on the type of resource. For example, ControlLogix controllers only support logical name-based security — a ControlLogix controller **must** have a logical name assigned.

For RSLogix 5 and 500 controllers, the logical name is associated with the relative path and not the physical controller.

PLC-5 and SLC 500 controllers support both path-based and logical name-based security.

What happens when you define a logical name?

If you define a logical name for a control device, the security system automatically uses the security permissions associated with that name, rather than with the device's network relative path, to determine access permissions. After defining a new logical name, you must also establish security permissions for the control device. Be sure to define an identical logical name for the control device on each computer on the network that has access to the device, if the different computers have different relative paths to the device.

If you configure security on a control device identified by a network relative path, and then later you define a logical name for the device, the original security permissions are not lost; they remain associated with the path, but

they do not transfer to the name. As a result, the original security permissions are no longer accessible, because security now attempts to access the security permissions using the name, not the path.

If you later change a control device's logical name, the original security permissions remain associated with the first logical name. You must re-define security permissions for the device, to associate them with the new logical name.

What happens when you undefine a logical name?

When you undefine a logical name, the security system automatically uses the security permissions associated with the device's network relative path.

The logical name and its associated security permissions still exist in the security system after a name is undefined. For example, suppose the name "MyPLC1" is assigned to Device1 on Computer A and Computer B, and each computer has a different relative path to Device1. When a user attempts to perform an action on Device1 from either computer, the security system checks the permissions associated with "MyPLC1."

Now suppose we undefine the name "MyPLC1" on Computer A, but leave it assigned on Computer B. If a user attempts to perform an action on Device1 from Computer A, security uses the permissions associated with the Device1's network relative path. If a user attempts to perform an action on Device1 from Computer B, however, security uses the permissions associated with the logical name "MyPLC1."

Do not undefine logical names for Logix5000 controllers. Because Logix5000 controllers do not have network relative paths, undefining a logical name can cause unexpected results. For details, see [Enable security for Logix Designer application](#) on [page 126](#)

Where to go from here

Do one of the following:

- Continue adding and configuring resource groups, if desired.
- Go to [RSLink and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLink software.
- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure projects.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components

- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.

RSLinux and FactoryTalk Security

This section discusses how you configure RSLinx® Classic to work with FactoryTalk® Security.

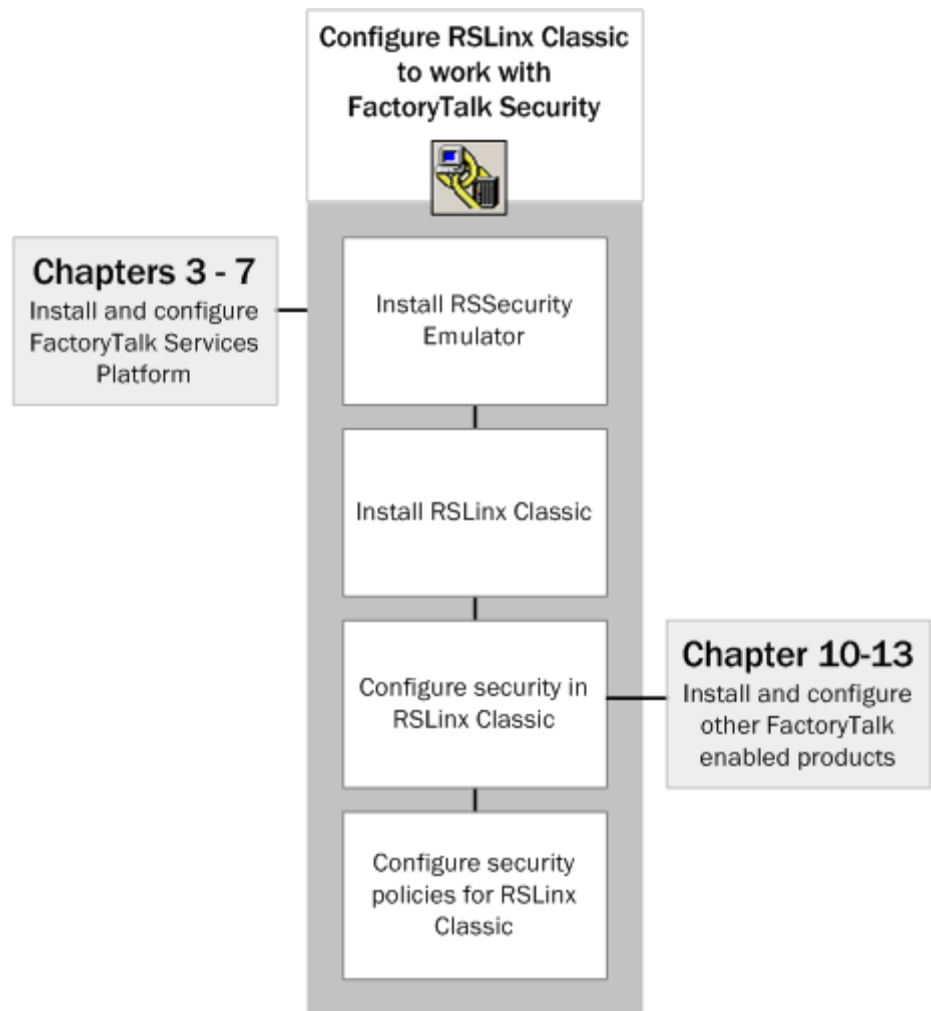
Before you begin

- Verify that you have installed and activated the software listed below under [What you need](#) on [page 113](#).
- FactoryTalk View installation disc or RSLinx Classic installation disc
- Become familiar with the terms and concepts of FactoryTalk Security. See [Understanding automation security](#) on [page 17](#) and [About the FactoryTalk system](#) on [page 21](#) for more information.

What you need

- FactoryTalk Services Platform v. 2.10 (CPR 9) or later. Using the newest available version is recommended.
- FactoryTalk Security (installed with FactoryTalk Services Platform)
- Identify FactoryTalk Network Directory to use during RSLinx and RSSECURITY Emulator installation

Follow these steps



Install the Rockwell Software Security Emulator

RSLinx 5000 software version 19 or earlier, uses the Rockwell Software Security Emulator to communicate with FactoryTalk Security. Starting with version 20, RSLinx 5000 obtains security information directly from FactoryTalk Services Platform and does not require RSecurity Emulator.

Follow these instructions to install the Rockwell Software Security Emulator if you are using RSLinx 5000 version 19 or earlier.

1. From the Start menu, select **All Programs > Rockwell Software > FactoryTalk Tools > RSecurity Emulator Install**.
2. Follow the installation prompts to complete the installation.

Important: For FactoryTalk Security to work, you must install RSecurity Emulator **before** you install RSLinx Classic.

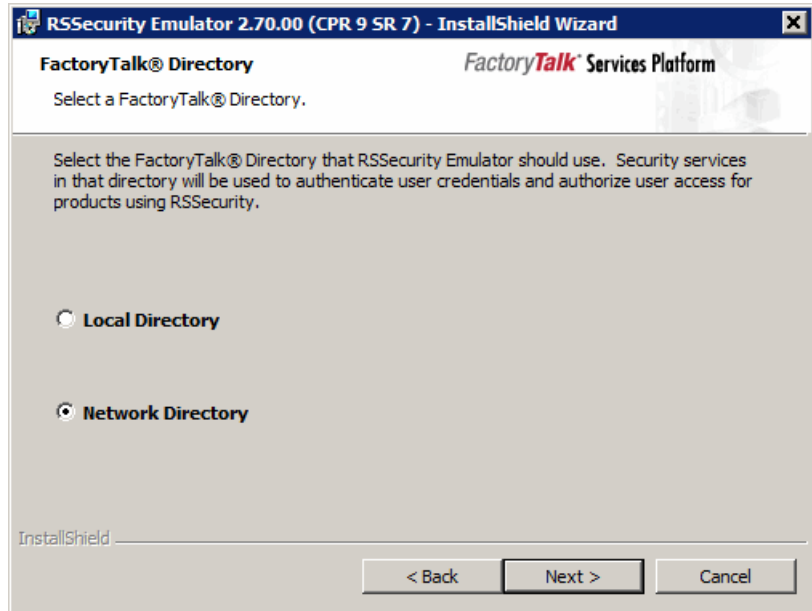
Follow these steps on every computer where RSLinx Classic will be installed:

1. From the disc of any FactoryTalk product, install the FactoryTalk Services Platform, if it is not already installed.

Important: All FactoryTalk products running on the same computer must use the same version of the FactoryTalk platform.

2. Specify the location of the FactoryTalk Network Directory:
 - If your FactoryTalk system is distributed across a network, specify which computer is hosting the FactoryTalk Network Directory Server. To do this, click **Start > All Programs > Rockwell Software > FactoryTalk Tools > Specify FactoryTalk Directory Location**, and then specify the name of the computer where the Network Directory Server is located.
 - If your FactoryTalk system is not distributed across a network and uses only the FactoryTalk Local Directory on this computer, skip this step.
3. Install the RSSecurity Emulator:
 - a. From the Windows **Start** menu, select **All Programs > Rockwell Software > FactoryTalk Tools > RSSecurity Emulator Install**.
 - b. On the Welcome screen, click **Next**.
 - c. Review and accept the end user license agreement, and then click **Next**.
 - d. In the **Customer Information** window, enter your information and then click **Next**.
 - e. In the **Setup Type** window, select the type of installation you want and then click **Next**.
4. Specify the appropriate FactoryTalk Directory:
 - a. In the FactoryTalk Directory window, select the directory for RSSecurity Emulator to use (select **Network Directory** for this example) and then click **Next**.

Tip: RSLinx Classic supports FactoryTalk Network and Local Directories. The configuration of the RSSecurity Emulator determines which FactoryTalk Directory RSLinx Classic will use.



Important: You must select the same FactoryTalk Directory used by any other FactoryTalk-enabled software installed on the computer.

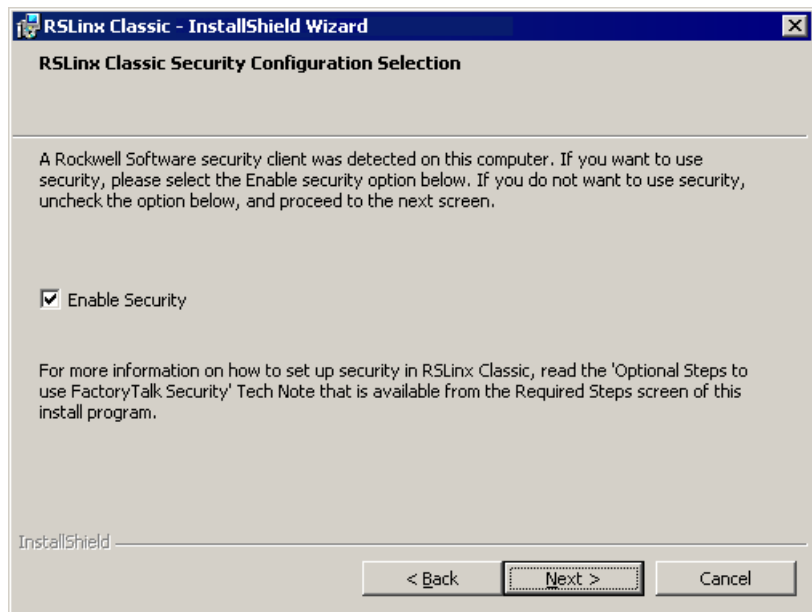
- b. When the installation is finished, click **Finish**. You do not need to do anything else to configure RSSecurity Emulator.

Configuring RSLinx Classic to work with FactoryTalk Security

With the RSSecurity Emulator installed, follow these steps to install and configure RSLinx Classic to work with FactoryTalk Security:

1. Place the RSLinx Classic installation disc in the appropriate drive. The installation program should start automatically.
2. In the RSLinx Classic Welcome page, click **Required Steps**.
3. In the Required Steps page, click **Install RSLinx Classic**.

- Follow the instructions until you come to the RSLinx Classic Security Configuration Selection page.

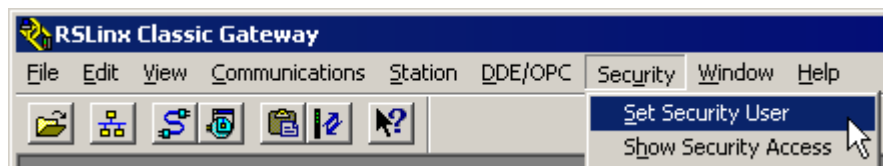


Important: The **Security Configuration Selection** dialog box displays only if the installation program detects RSecurity Emulator.

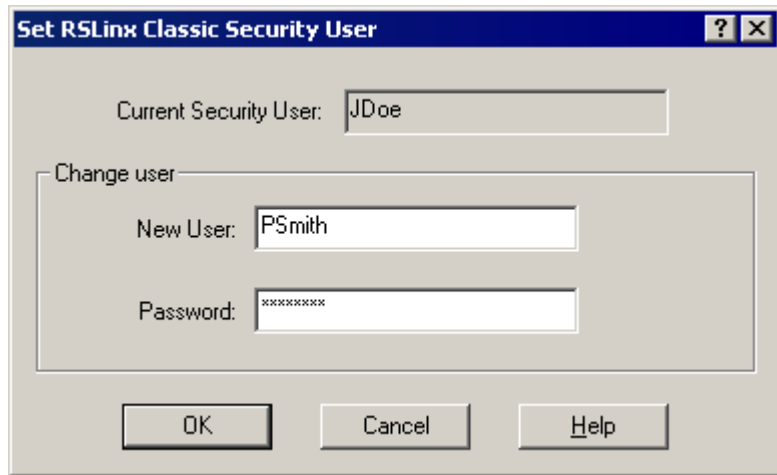
- Select the **Enable Security** check box and click **Next**.
- Follow the instructions to complete the installation.

Configure security for RSLinx Classic

- Open RSLinx Classic from **Start > All Programs > Rockwell Software > RSLinx > RSLinx Classic**.
- Select **Set Security User** from the **Security** menu.



3. In the **Set RSLinx Classic Security User** dialog box, type the user name and password of an authorized FactoryTalk user, and then click **Ok**. (In this example we used **PSmith**, the user we created in FactoryTalk Administration Console.



Tip: Because access to features in RSLinx Classic is governed by the permissions you set for a user in FactoryTalk Administration Console, some features out of the 13 securable features in RSLinx Classic may be inaccessible (for example, if the user you entered does not have the appropriate permission).

Assigning permissions

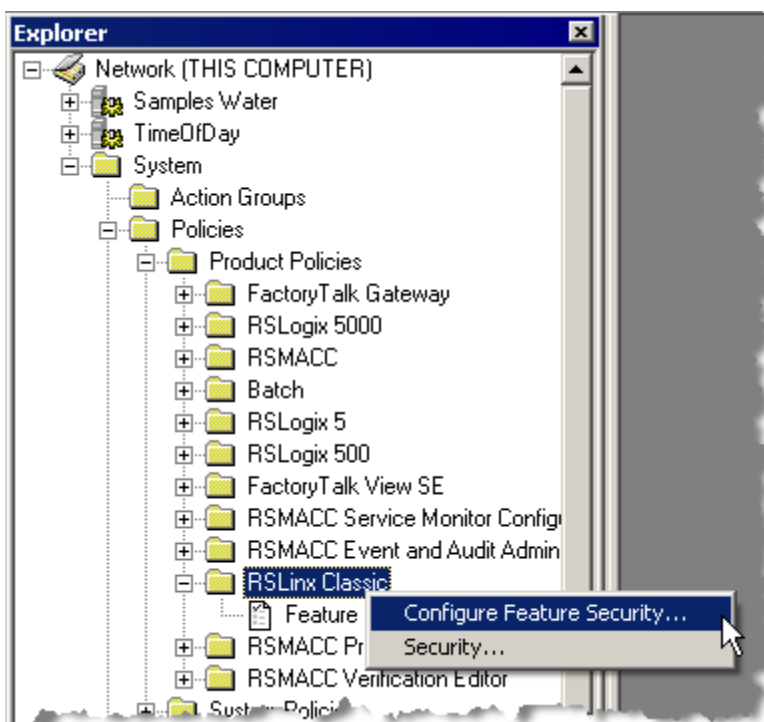
You can restrict access to the features of individual FactoryTalk products in your system to prevent inadvertent changes or tampering. Only users with the required level of access can use the product features you have secured.

For example, when you set up product policies for RSLinx Classic, you might restrict the ability to shut down the RSLinx Classic service to a small group of users, to prevent parts of your automation system from going down at runtime.

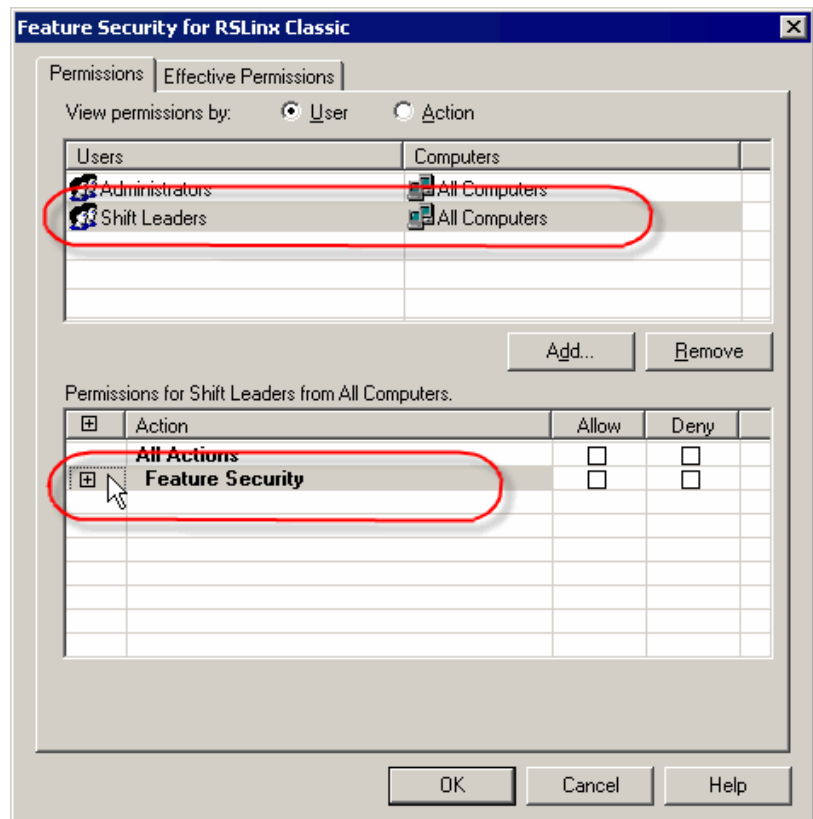
Each FactoryTalk product you install provides different securable features. See the individual product documentation for details.

Before you follow the steps below, you must create a user group by the name **Shift Leaders**, and give the Shift Leaders group access to all common actions. For information on how to create a user group and assign permissions to it, see [Create a user group](#) on [page 74](#), and [Assigning permissions](#) on [page 83](#)

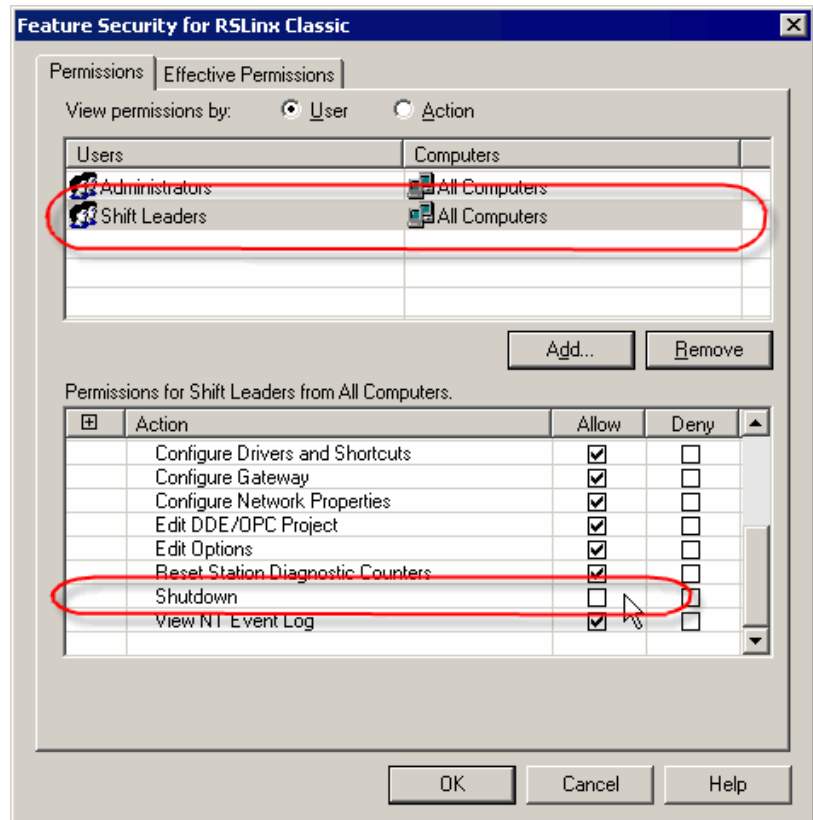
1. From the Explorer, expand **System > Policies > Product Policies > RSLinx Classic**, and then select **Configure Feature Security** from the pop-up menu.



- From the **Permissions** tab on the **Feature Security** dialog box, select the **Shift Leaders** group to highlight it. (If you don't see the Shift Leaders group, click the **Add** button, select the **Shift Leader** group, and then click **OK**.)
- In the Permissions for Shift Leaders from All Computers area, select the **Allow** check box next to **All Actions**.
- Expand the **Feature Security** list by clicking the plus sign (+), as shown here.



- Scroll down the list to **Shutdown** and clear the **Allow** check box for Shutdown. This prevents anyone in the Shift Leaders group from shutting down RSLinx Classic.

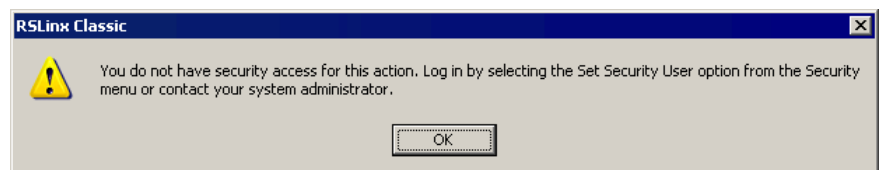


- Click **OK** to save and close the dialog box.
2. Test the permissions:

- Open **RSLinx Classic** from **Start > All Programs > Rockwell Software > RSLinx > RSLinx Classic**
- Select **Set Security User** from the **Security** menu. Make sure that **PSmith** is still the current security user. If not, log in as **PSmith** with a password of **password**, and then click **OK**.



- Now select **Exit** from the **File** menu. You should see the following message:



3. (Optional) Log back in as a FactoryTalk user with administrative rights and continue testing the various feature and policy security settings for RSLinx Classic.

Considerations when using RSLinx Classic with FactoryTalk Security

- **Network/Local Directory**

The FactoryTalk Services Platform can install two completely separate and independent FactoryTalk Directories: a Local Directory and a Network Directory. User accounts, passwords, and security permissions to securable features are completely separate and cannot be shared between the Network Directory and the Local Directory. Configuring any of these items on one directory does not configure them on the other. Similarly, changing the password to a user account in one directory does not change the password the other directory, even if the account has the same name in both directories.

When configuring RSLinx Classic to work in one of the two directories, please keep the following in mind:

- RSLinx Classic security policies and RSSecurity Emulator must be installed in the same directory (either Local or Network).
- If you configured RSLinx Classic to work in Local Directory and want to use FactoryTalk Security, remember that when working in Local directory you can administer security only on a single computer.
- If you did not select the "Enable Security" option during RSLinx Classic install, but want to enable security now, you must uninstall and then reinstall RSLinx Classic.
- Every time you run RSLinx Classic, be sure to verify that the user name displayed in the Current Security User box of the **Set Security** dialog box (**Security > Set Security User**) is correct. If it is incorrect, enter the new user name and password, and then click **OK**.

What can I secure in RSLinx Classic?

The following table explains the features you can restrict access to in RSLinx Classic. For example, you might restrict the ability to shut down the RSLinx Classic service to a small group of users, to prevent parts of your automation system from going down at runtime.

Securable feature	Description
Clear DDE/OPC Event Log	Displays information on any DDE/OPC error messages logged while running RSLinx Classic with DDE/OPC compliant programs.
Configure CIP Options	Administers how PCCC requests that use the CIP protocol are sent over networks.
Configure Client Applications	Maps configured and running RSLinx Classic drivers to legacy INTERCHANGE C API, as well as displays the link identifier of the virtual network maintained by RSLinx Classic for the use of Client Applications in the virtual link unsolicited messaging model.
Configure ControlLogix Gateway	Provides you with information about the modules in your ControlLogix Gateway.
Configure DDE/OPC Topic	Configures DDE/OPC topic.
Configure Drivers and Shortcuts	Configures (add, edit, or delete) drivers and shortcuts that allow RSLinx Classic to communicate with your PLC, as well as provide quick access to specific networks.
Configure Gateway	Allows you to enable the RSLinx Classic Gateway.
Configure Network Properties	Allows you to configure network properties.
Edit DDE/OPC Project	Allows you to edit your DDE/OPC project.
Edit Options	Displays the options dialog box which contains the General and DDE tabs.
Reset Station Diagnostic Counters	Clears the counters in the station diagnostic screens.
Shutdown	Shuts down RSLinx Classic.
View NT Event Log	Records important system occurrences such as RSLinx Classic drivers successfully starting and stopping.

For more information on securable features, refer to the RSLinx Classic Help.

Where to go from here

Do one of the following:

- Continue assigning permissions for RSLinx Classic actions, if desired.
- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure projects and devices like Logix5000, PLC, and SLC controllers.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components
- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.

Logix Designer application and FactoryTalk Security

This section describes how to configure the Logix Designer application for use with FactoryTalk® Security so that you can secure access to your controllers, projects, and controller resources.

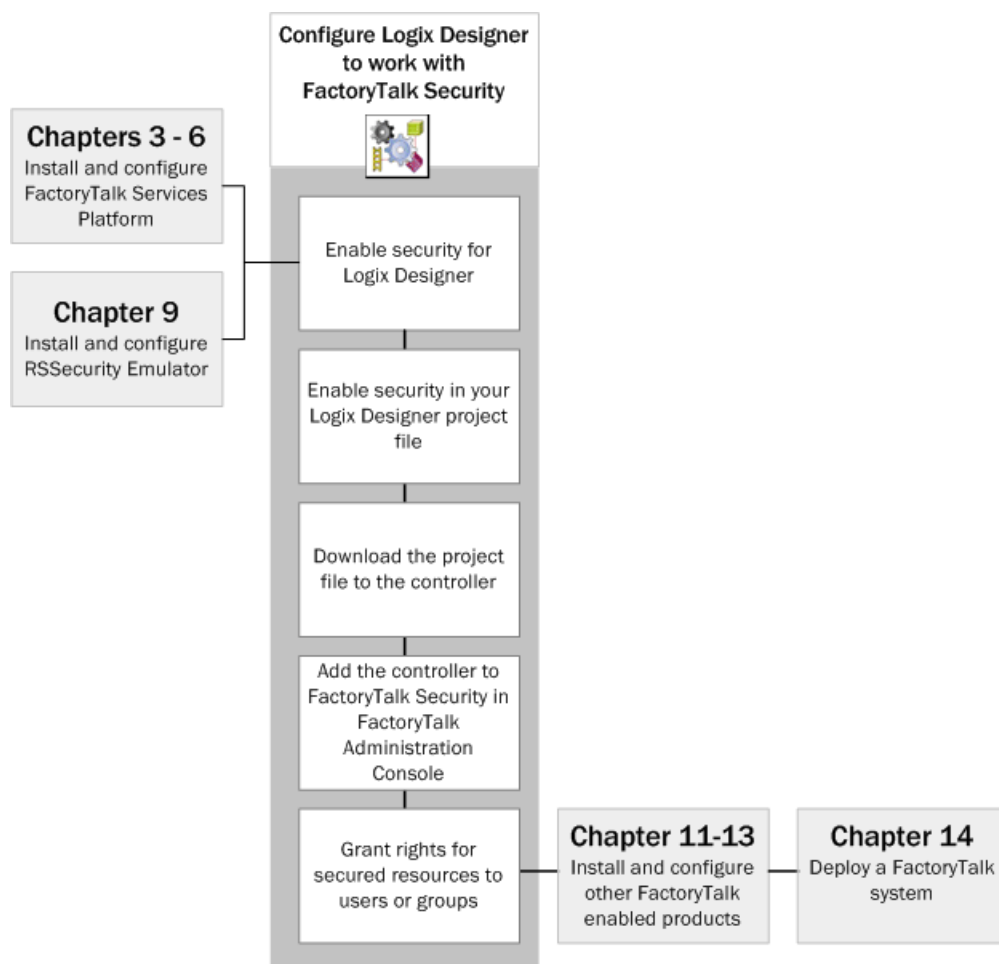
Before you begin

- Verify that you have installed and activated the software listed below under [What you need](#) on [page 125](#).
- Verify that the Logix5000™ firmware has been updated to version 16 or later.

What you need

- FactoryTalk Services Platform 2.10 or later. Using the newest available version is recommended.
- Logix5000 controller with firmware updated to version 16.0 or later
- Studio 5000 installation CD. Using the newest available version is recommended.
- RSSecurity Emulator if you are using RSLogix 5000 version 19 or earlier (see [Install the Rockwell Software Security Emulator](#) on [page 114](#) for additional information)
- RSLinx® Classic 2.53 or later, installed and with security enabled. See [RSLinx and FactoryTalk Security](#) on [page 113](#).

Follow these steps

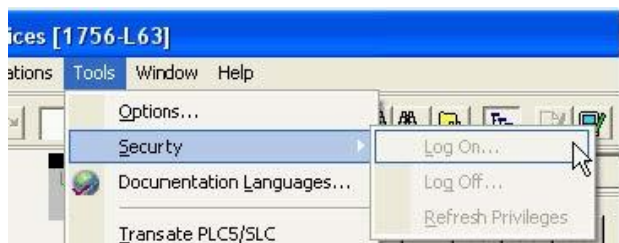


Tip: When managing large numbers of users and controllers, group users with user groups, group permissions with action groups, and use the Resource Grouping method to secure your resources to simplify administration of permissions. See [Create a user group](#) on [page 74](#), [Creating action groups](#) on [page 87](#), and [Resource grouping](#) on [page 103](#) for more information.

The following sections in this chapter show how to set permissions for an individual user on a single controller.

Enable security for Logix Designer application

If the Security menu appears dimmed, as shown in this picture, you need to enable security for Logix Designer application.

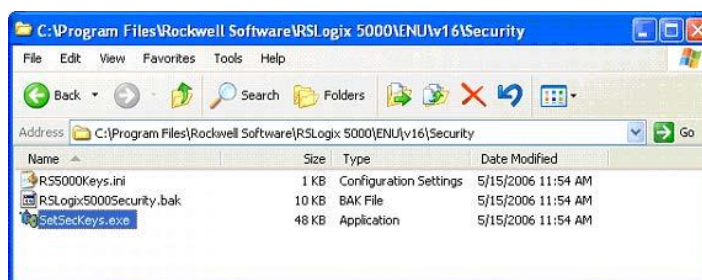


If the security menu appears dimmed, you need to install FactoryTalk Services Platform. See [Install FactoryTalk Services Platform](#) on [page 28](#). If you are using the application with version 20 or later and the security menu is enabled, skip to [Enable security for Logix Designer application](#) on [page 126](#).

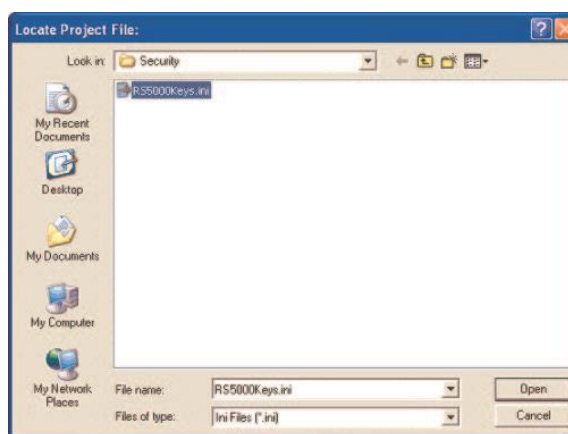
If you are using RSLogix 5000 software version 19 or earlier, you need to use **SetSecKeys** to enable security. Follow the instructions below.

1. For RSLogix 5000 software v19 or earlier, the SetSecKeys software is added to the system during the RSLogix 5000 software installation.

Navigate to: **Program Files\Rockwell Software\RSLogix 5000\ENU\vx\Security** and double-click SetSecKeys.exe. For this example, we are using RSLogix 5000 software v16.



2. If prompted to locate the project file, select the RS5000Keys.ini file and click Open.





For RSLogix 5000 software version 19 or earlier, if you need to disable FactoryTalk Security for RSLogix 5000 software, please contact Rockwell Automation Technical Support.

3. In the Enable/Disable Security Keys dialog box, select the **RSLogix 5000** check box and then click OK.



4. If the **Security: Enable** dialog box appears, click OK.
5. Open the FactoryTalk Administration Console:
 - a. Click **Start > All Programs > Rockwell Software > FactoryTalk Administration Console**.
 - b. Select the FactoryTalk Directory option and click OK.

Important: Starting with version 20 of the application, security settings are obtained from the FactoryTalk Network Directory. RSSECURITY Emulator is not required and the FactoryTalk Local Directory is not supported.

- c. If prompted to log on to FactoryTalk, enter your FactoryTalk user name and password, and then click OK.

Tip: In FactoryTalk Security CPR 9 or later, single sign-on is enabled by default so you are not typically prompted to log on to FactoryTalk. When single sign-on is enabled, you may still be prompted to log on if you are switching from a Local to Network directory or you are not logged on as an administrator. If you are upgrading from CPR 7 or you changed the default FactoryTalk security configuration, you will be prompted to log on. If you cannot log on to FactoryTalk, see "I cannot log on to FactoryTalk" in FactoryTalk Security Help. See also "Set up security policies" and "Add a computer account" in FactoryTalk Security Help.

6. Open the RSLogix 5000 Feature Security Properties dialog box:
 - a. In the Explorer window, navigate to: **System > Policies > Product Policies > RSLogix 5000**.
 - b. Right-click Feature Security and select Properties.

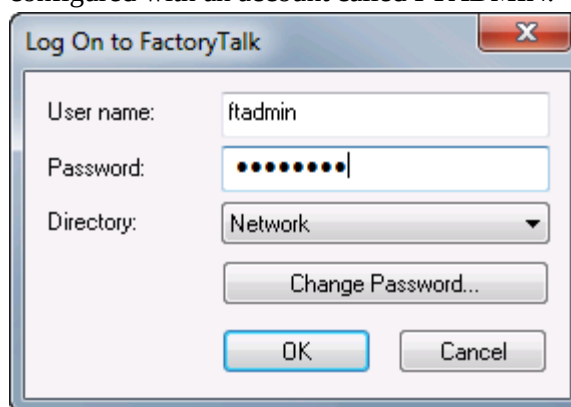
7. Secure the controller:
 - a. In the Feature Security Properties dialog box, select **Controller:Secure** and then click Browse.
 - b. In the Configure Securable Action dialog box, click Add to select the user accounts or groups that you want to configure.
 - c. In the Select User and Computer dialog box, select the user accounts or groups and click OK.
 - d. Follow the instructions to complete the configuration.

Secure a Logix Designer Project File

After you configure the Logix Designer application to be security aware, the next step is to enable security in a project file. Follow these steps to secure a project file.

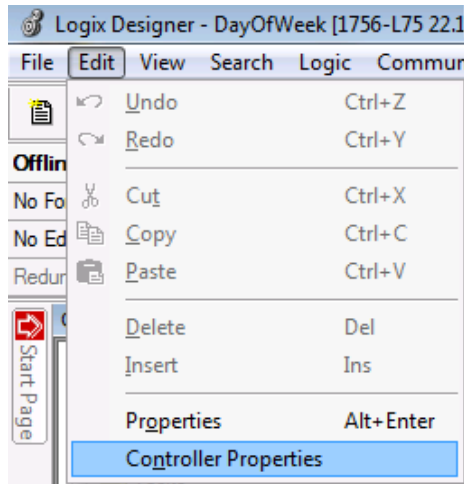
1. Open Logix Designer.
 - a. Click the **Start** button, then click **All Programs**, then click **Rockwell Software**, and then click **Studio 5000**.
 - b. If prompted to **Log On to FactoryTalk**, type your FactoryTalk **User name** and **Password**, and then click **OK**.

In the example below, the FactoryTalk Directory (FTD) was configured with an account called FTADMIN.



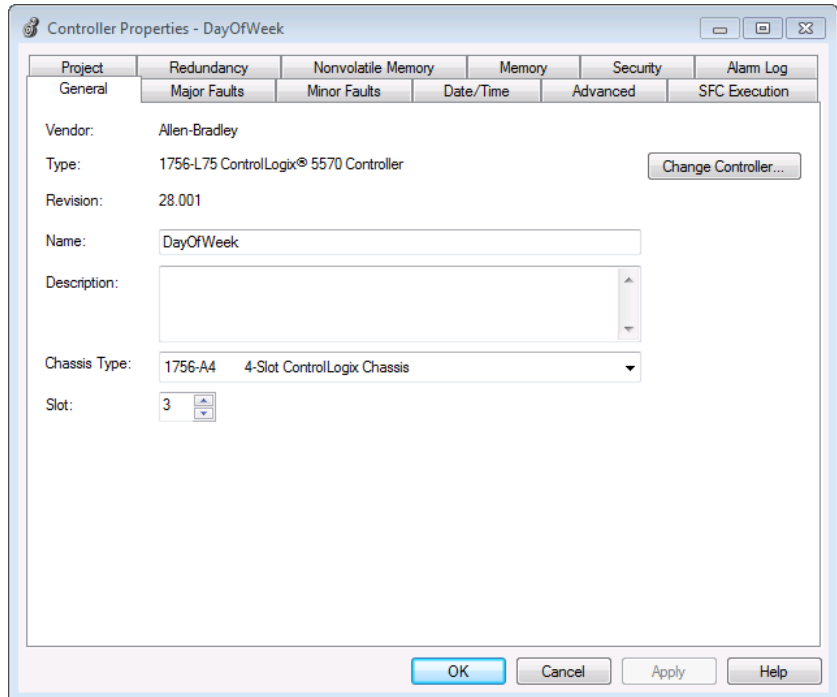
2. Open the project file that you want to secure. This example uses the DayOfWeek project file, which is installed with the software. From the Menu bar, click **Help**, then click **Vendor Sample Projects**. On the **Quick Start** screen, click **Open Sample Projects**, and then find the **DayOfWeek.ACD** file. Click the **DayOfWeek.ACD** and then click **Open**.

3. On the menu bar, click **Edit**, and then click **Controller Properties**.



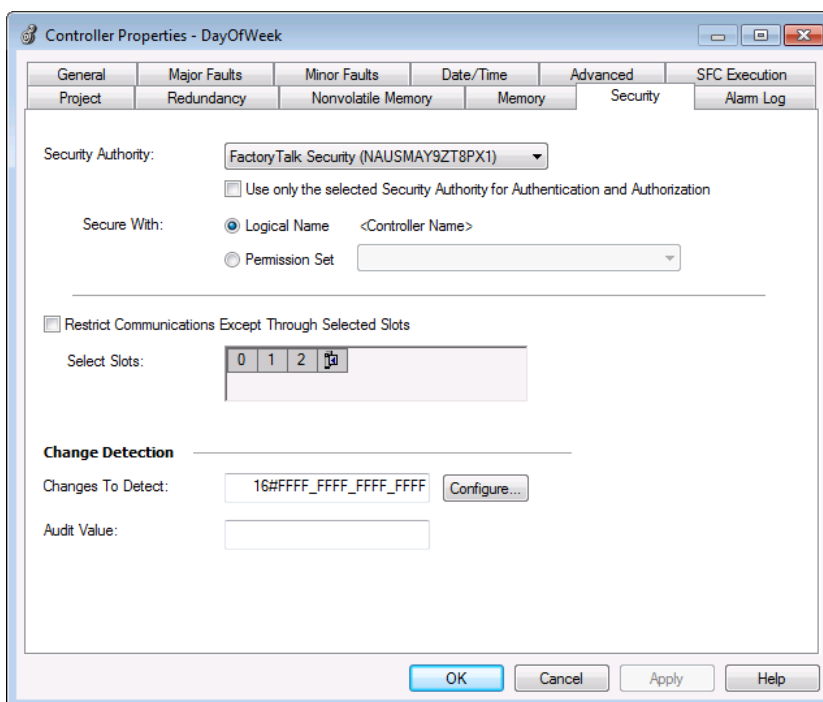
4. Click the General tab to find the controller name. Write down the name that appears in the Name field. By default, this is the name of the ACD file that will be used later on Apply Security to a Controller Resource when setting security in the FactoryTalk Administration Console.

In this example, the name is **DayOfWeek**.



5. Click the **Security** tab to configure the security settings.

Tip: If the **Security** tab does not appear in the **Controller Properties** dialog box, click the **Advanced** tab. In the **Security** box, select **FactoryTalk Security**.



6. In the **Security Authority** list, select **FactoryTalk Security**. By default, users do not have the **Controller: Secure** privilege that is required to select FactoryTalk Security as the Security Authority. If you cannot select this setting, check the FactoryTalk Administration Console to make sure you have the **Controller: Secure** privilege.

Important: When you select a security authority for a project, you can only access the project and any controller that contains it when you have been granted access in FactoryTalk Security.

7. To associate the project with a specific authority, select the **Use only the selected Security Authority for Authentication and Authorization** check box. When this check box is selected, users interacting with this project must be authenticated and authorized by either the primary or the secondary Security Authority.

Important: Before you associate this project with a specific Security Authority, we recommend that you back up the FactoryTalk Directory and save unsecured versions of this project file in (.ACD) or (.L5X or .L5K) formats. For details about backing up a FactoryTalk Directory, see the FactoryTalk Help:
Start > Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Help

Tip: The check box is available when you are using FactoryTalk Services Platform 2.50 or later and a version of the application that supports associating a project with a specific Security Authority.

8. Select a **Secure With** option:

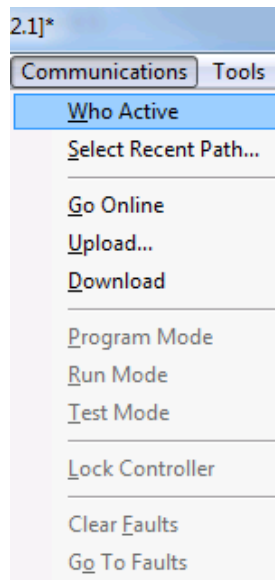
- To associate the project with a Logical Name in the FactoryTalk Administration Console, select **Logical Name <Controller Name>**. If there is no existing Logical Name that matches the controller name, a new Logical Name is created with the controller's name.
- To associate the project with a Permission Set configured in the FactoryTalk Administration Console, select **Permission Set** and select a permission set from the list.

9. Click **OK**. If prompted to confirm the controller settings, click **Yes**.

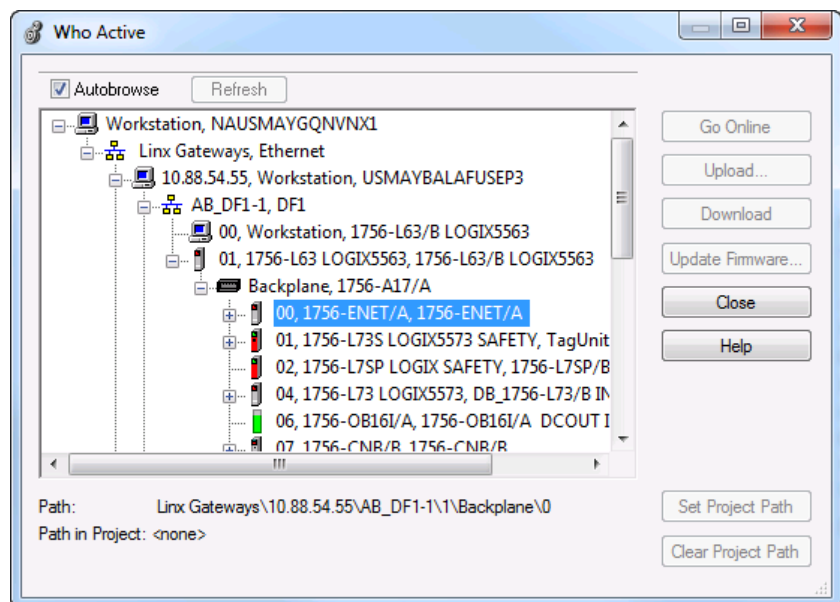
Important: When you select a security authority for a project, you can only access the project and any controller that contains it when you have been granted access in the FactoryTalk Administration Console.

10. Save the project file.

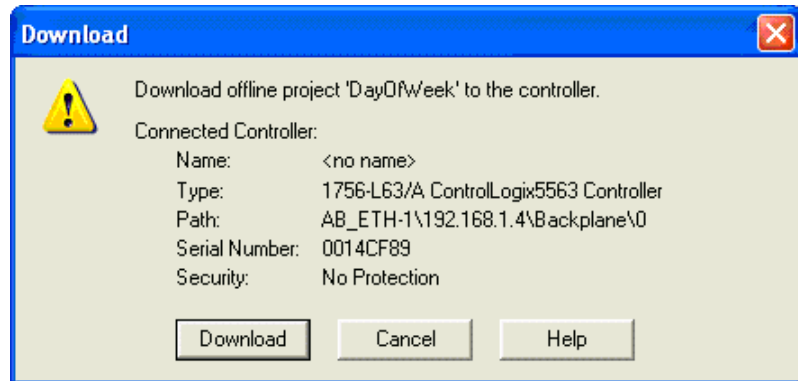
11. On the menu bar, click **Communications**, and then click **Who Active** to download the project file to the controller.



12. In the **Who Active** window, locate and select the controller resource.



13. Click **Download** to continue.



Secure a Logix Designer project component

In addition to securing Logix Designer projects, you can also secure individual tags, routines, and Add-On Instructions with additional or different permissions. For example, you can apply permissions that allow a user to modify some tags, but not others. The security settings that you apply to a specific component override any security policy applied to the overall project.

Keep the following considerations in mind when applying permission sets to components:

- Permission sets can be applied only when the overall project has been secured.
- A permission set that restricts viewing an Add-On Instruction or routine in the Logix Designer application does not prevent a user from exporting and viewing the Add-On Instruction or routine in clear text. To prevent exporting the component, configure the permission set to deny the **Project: Export** permission.
- To apply a permission set to a component, users must have **Component: Modify Permission Set** privilege, which is configured in the FactoryTalk Administration Console.
- The permission set that you apply to a component overrides the permissions applied to the entire project.

To apply a permission set to a tag:

1. In the **Tag** editor, select a tag.
2. Point to the **Properties** pane on the right side of the **Tag** editor. Click  to pin the **Properties** pane to the dialog box.
3. In the **Permission Set** control, select the permission set to apply to the tag. The permission set is applied immediately when you select it.

To apply a permission set to a routine:

1. In the **Controller Organizer** or the **Logical Organizer**, right-click the routine and select **Properties**.
2. In the **Routine Properties** dialog box, in the **Permission Set** control, select a permission set to apply.
3. Click **OK**.

To apply a permission set to an Add-On Instruction:

1. In the **Controller Organizer** or the **Logical Organizer**, right-click the Add-On Instruction and select **Properties**.
2. In the Add-On Instruction **Properties** dialog box, in the **Permission Set** control, select a permission set to apply.
3. Click **OK**.

Configure a Secondary Security Authority

When a project is protected by a primary security authority, you can configure a secondary security authority. The secondary security authority further restricts Guest Users beyond the permissions granted by the primary security authority. For example, an original equipment manufacturer (OEM) can secure a project with FactoryTalk Services Platform using a primary directory, and an end customer can further secure the project with their own FactoryTalk Services Platform directory.

Tip: A secondary security authority cannot grant permissions that are denied by the primary security authority.

When a project is protected by a primary security authority, the following message appears at the top of the **Controller Properties dialog box - Security tab** when you are a Guest User:

This project is secured by a Primary Security Authority, limiting permitted actions. Additional security is configured here.

To configure a secondary security authority:

1. In the **Controller Organizer**, right-click the project name at the top of the pane and select **Properties**.
2. In the **Controller Properties** dialog box, click the **Security** tab.
3. In the Security Authority box, select FactoryTalk Security.
4. To associate this project with a specific Security Authority, select the **Use only the selected Security Authority for Authentication and Authorization** check box. When this check box is selected, users

interacting with this project must be authenticated and authorized by either the primary or the secondary Security Authority.

Important: Before you associate this project with a specific Security Authority, Rockwell Automation recommends that you back up the FactoryTalk Directory and save unsecured versions of this project file in (. ACD) or (.L5X or .L5K) formats. For details about backing up a FactoryTalk Directory, see FactoryTalk Help:
Start > Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Help.

When this check box is selected for the Secondary Authority, it does not cache additional Guest User permissions from the Secondary Authority within the project. Only Guest User permissions from the Primary Authority are stored within the project.

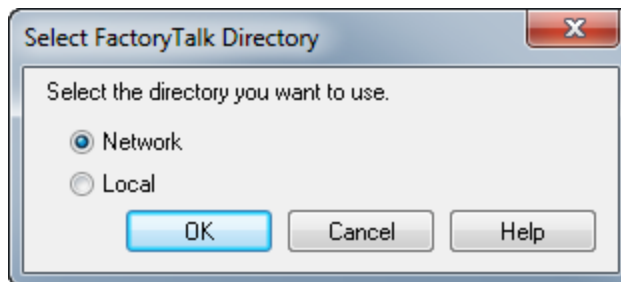
5. Click **OK**.

Apply security to a controller in FactoryTalk

The following steps show configuring a single controller for security. When managing large numbers of users and controllers, Rockwell Automation recommends that you group users with user groups, group permissions with action groups, and use the Resource Grouping method to secure your resources to simplify administration of permissions. You can also apply settings to multiple controllers by configuring and using permission sets. For details see the FactoryTalk Help: Click the **Start** button, then click **All Programs**, then click **Rockwell Software**, then click **FactoryTalk Tools**, and then start **FactoryTalk Help**.

Follow these steps to apply security to a specific controller.

1. Click the **Start** button, then click **All Programs**, then click **Rockwell Software**, and then click **FactoryTalk Administration Console**.
2. In the **Select FactoryTalk Directory** dialog box, click **Network** or **Local**, and then click **OK**.

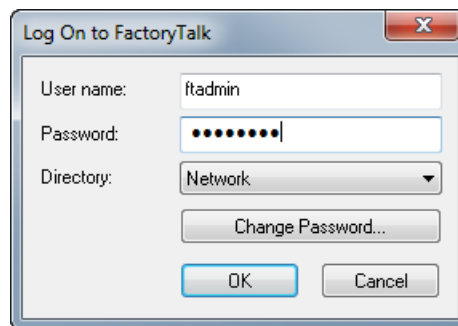


- For version 20 or later of the application, security settings are obtained from the FactoryTalk Network Directory. RSSECURITY Emulator is not required and the FactoryTalk Local Directory is not supported.
- The default FactoryTalk Security configuration has Single Sign On enabled, so that you will not be prompted to log on to FactoryTalk.

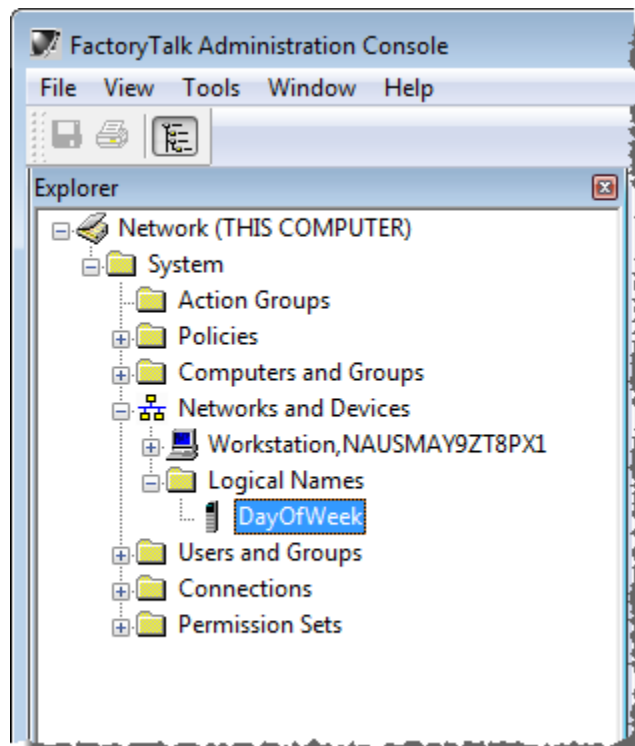
Customers upgrading from revisions prior to 16.03 or customers that have modified the default FactoryTalk Security configuration will be prompted to log on to FactoryTalk.

3. If prompted to log on to FactoryTalk, type your **User name** and **Password**.

In the example below, the FactoryTalk Directory (FTD) was configured with an account called FTADMIN.

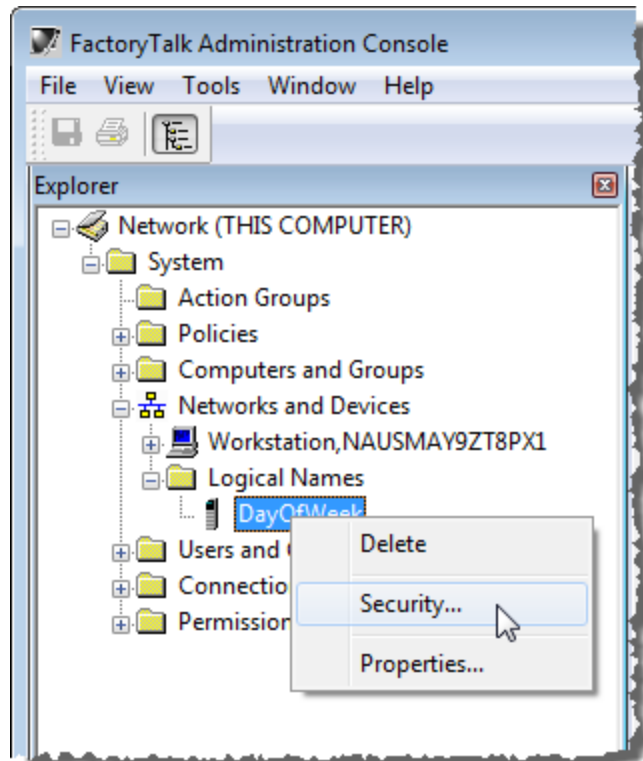


4. In the **Explorer** pane, find the Logical Name that matches the controller name. Expand **Networks and Devices** and expand **Logical Names**.

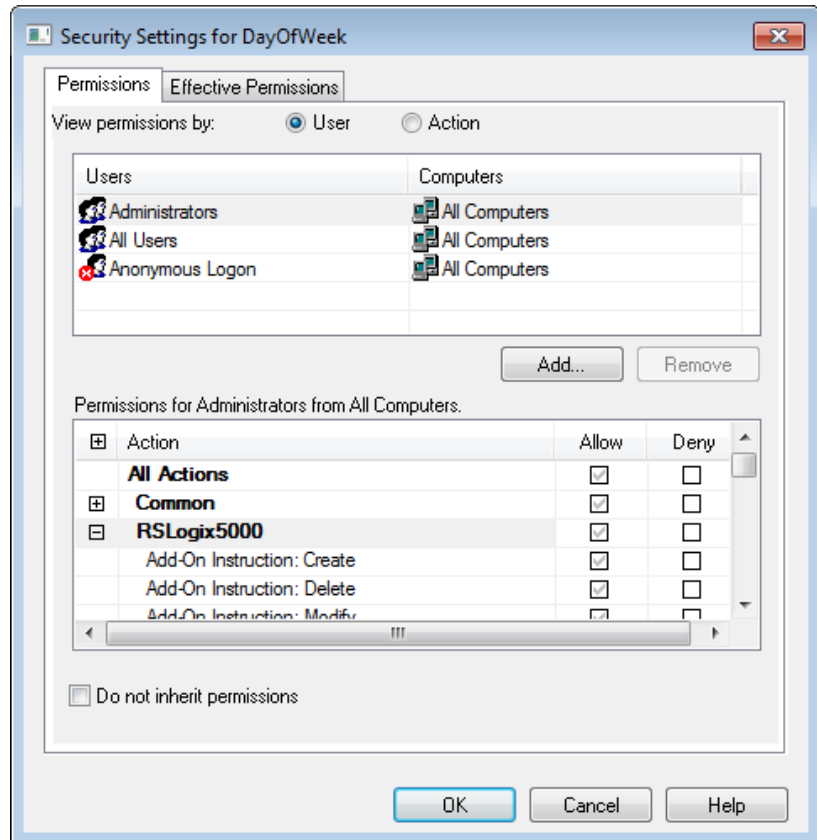


Tip: To configure security settings to be inherited by all controllers, right click **Networks and Devices** and click **Security**. From the **Security Settings** dialog box, you can configure security settings that are inherited by all secured projects. You can still configure unique permissions on a particular device, if needed.

5. Right-click the Logical Name that matches the controller and click **Security**.



6. In the **Security Settings** dialog box, configure security permissions for a particular user or user group and computer names.

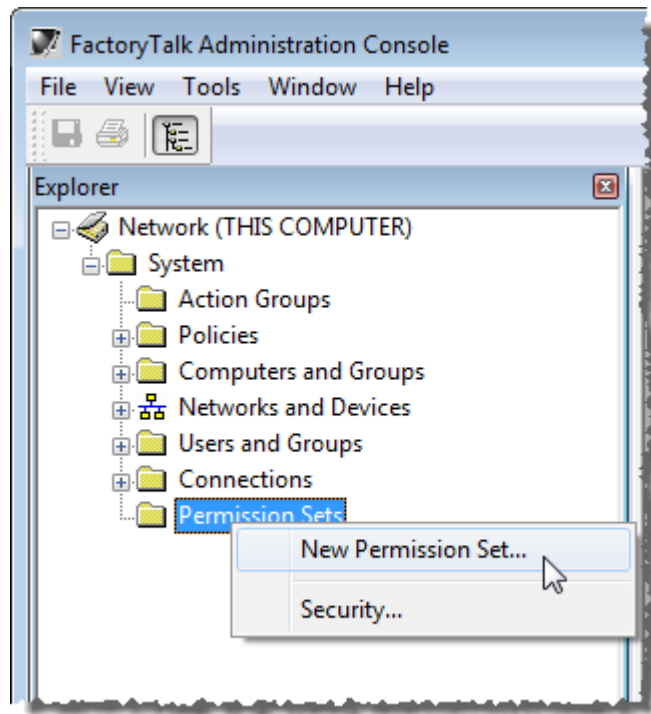


Configure a permission set for use in Logix Designer

Follow these steps to configure permission sets that you can apply to projects and project components in the Logix Designer application.

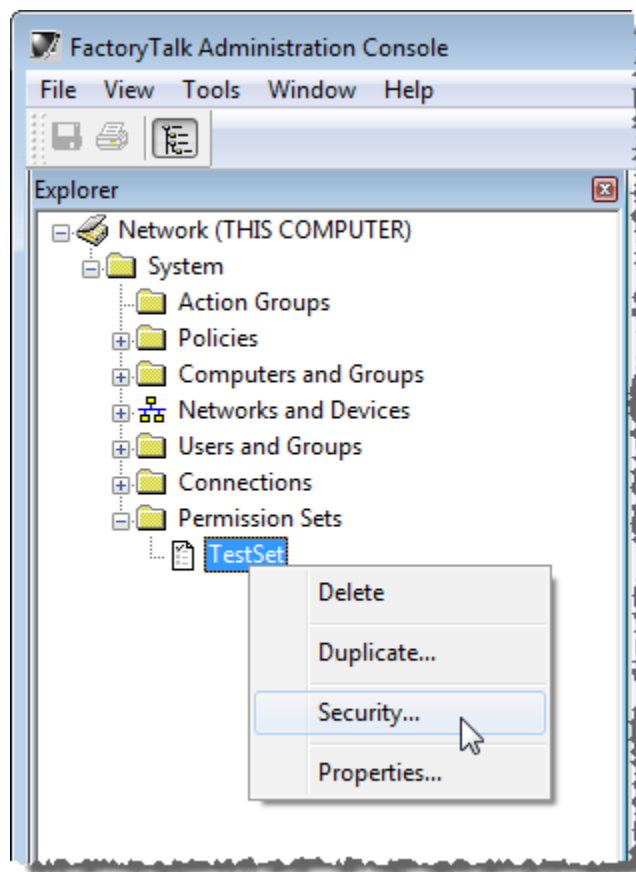
1. Open the FactoryTalk Administration Console.

2. In the **Explorer** pane, right-click **Permission Sets** and click **New Permission Set**.



3. In the **New Permission Set** dialog box, type a name and an optional description for the permission set and click **OK**. The new permission set appears in the Explorer pane.

4. Right-click the permission set and click **Security**.



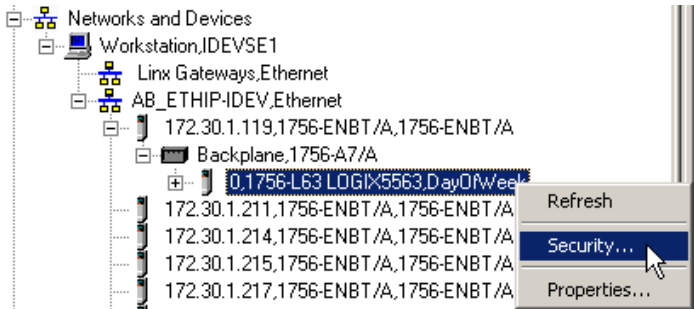
5. In the **Security Settings** dialog box, configure permissions for a particular user or user group and computer names.
6. Open the Logix Designer application. The permission set that you created appears in the **Permission Set** menus, and you can apply it to projects and project components.

Give access to secured controller resources

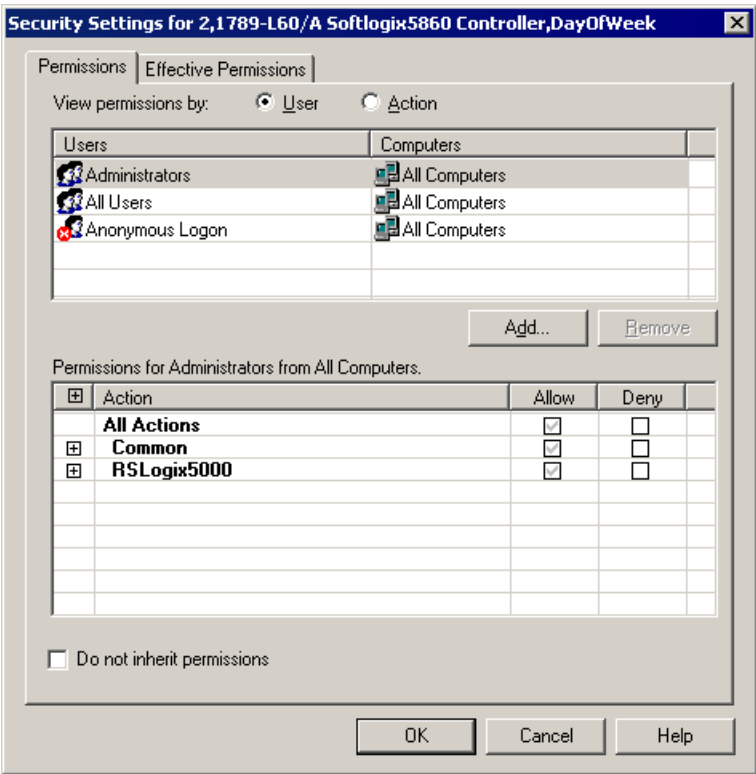
Now that you have set up security for the controller, you need to set up individual user or group permissions to control access to the secured Controller resources. For this example, we are going to give access to Pat Smith, a shift leader.

Tip: Use the Resource Grouping method to secure your resources. Rather than assigning security individually to each resource in the Networks and Devices tree, group related hardware into an application or area and then apply security to them. This allows you to assign the same permissions to hardware resources in one step rather than assigning them separately for each resource. For more information, see [Resource grouping](#) on [page 103](#).

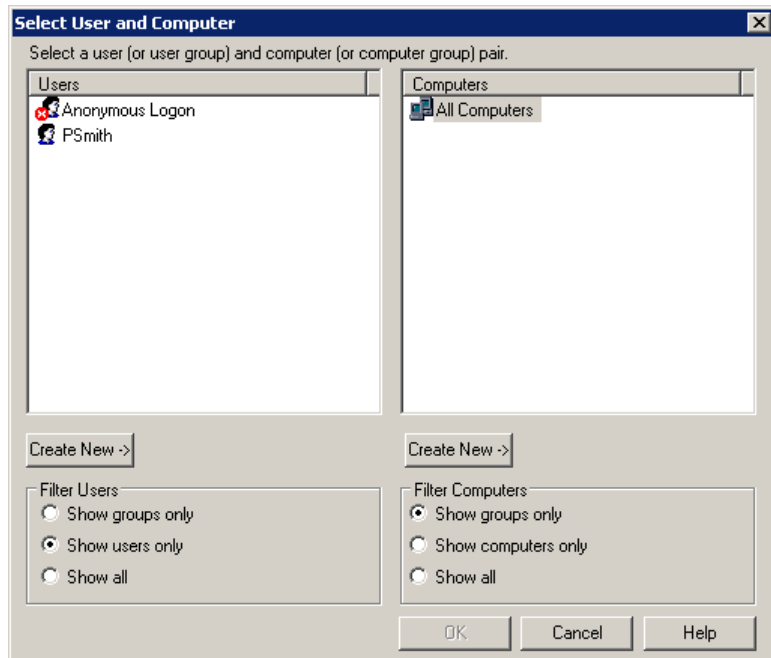
1. In FactoryTalk Administration Console, right-click the controller resource you added above, and then click **Security** on the pop-up menu.



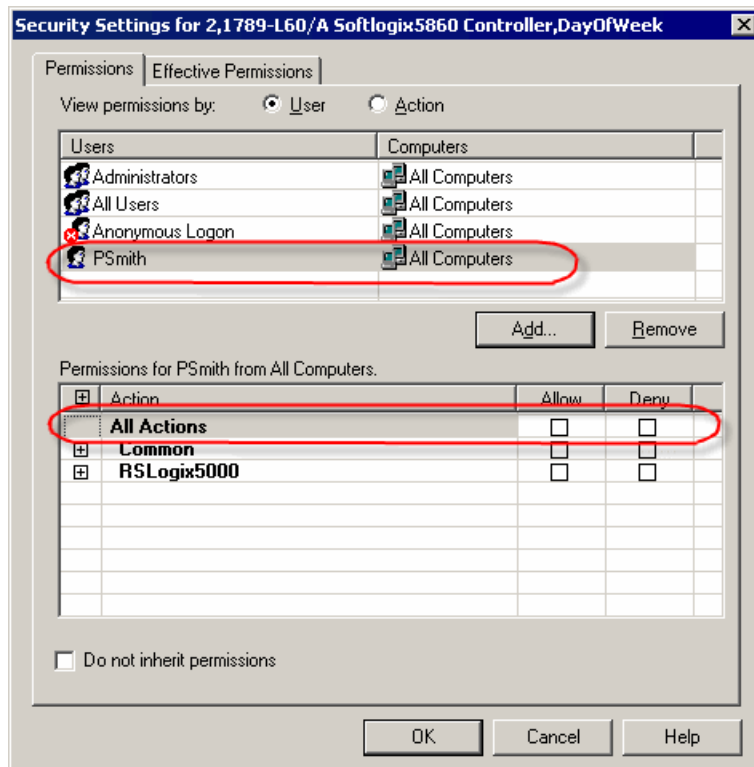
2. In the **Security Settings** dialog box, click the **Permissions** tab.



3. Click **Add**. The **Select User and Computer** dialog box opens.

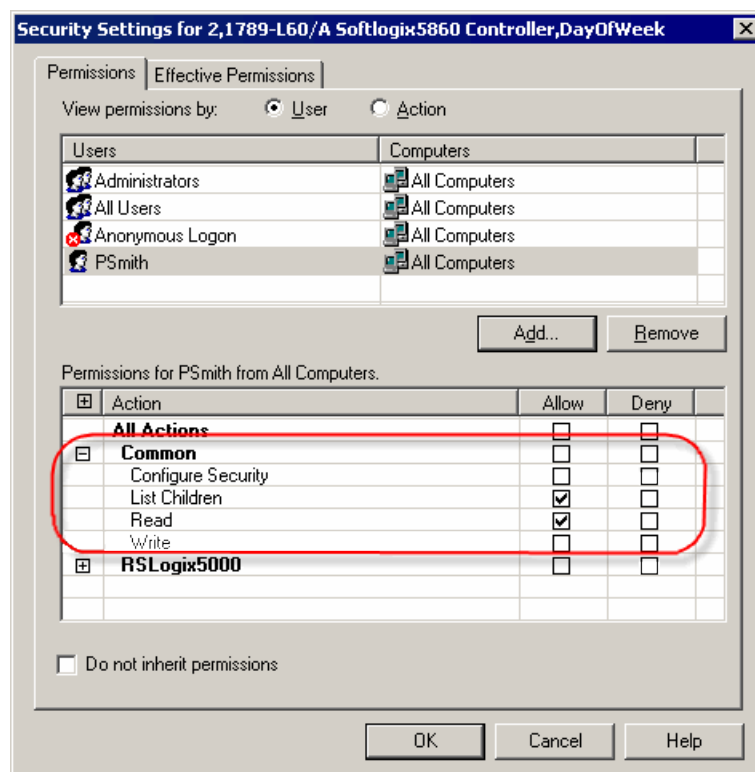


4. Select the **Show users only** option, select **PSmith** from the list of users, and then click **OK**. In the list of permissions for PSmith, make sure to clear the **Allow** check box that corresponds to **All Actions**.



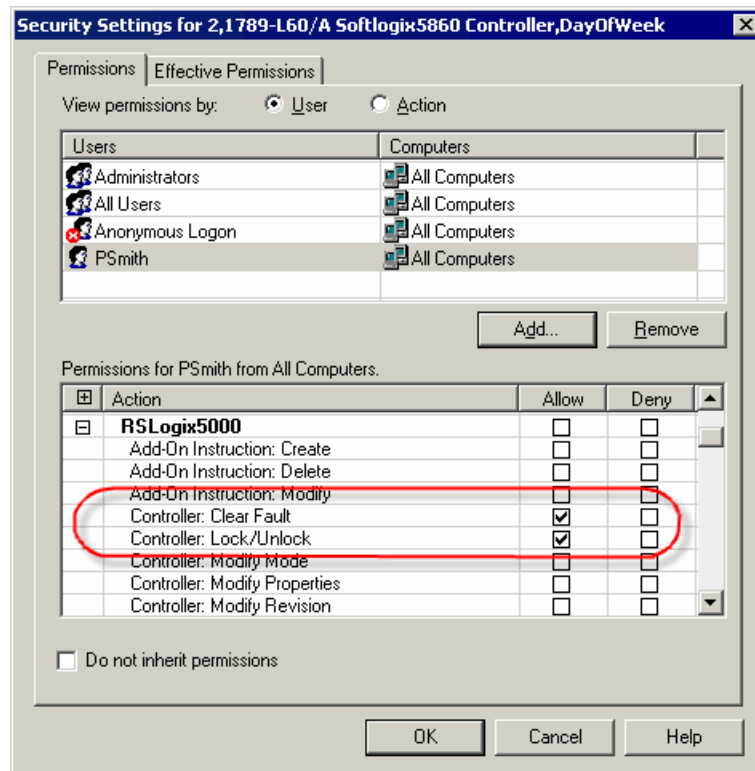
Tip: Wherever possible, remove **Allow** permissions instead of assigning explicit **Deny** permissions. This makes administration simpler because of the order of precedence of explicit permissions over inherited permissions, and Deny permissions over Allow permissions. Use action groups to group actions together and then assign security permissions to all of the actions in the group. This allows you to grant or deny permissions for a set of actions in one step, rather than having to set permissions for each action separately. [See Creating action groups2](#) on [page 87](#) for more information.

5. In the list of permissions, select the check boxes that correspond to the actions you want to allow or deny.
 - a. Click the plus sign (+) next to **Common** to display the common actions.
 - b. Select the **Allow** check boxes for **List Children** and **Read**. PSmith can view the controller resource, navigate through the Explorer view, read and write to project files, but cannot change the security for the device.



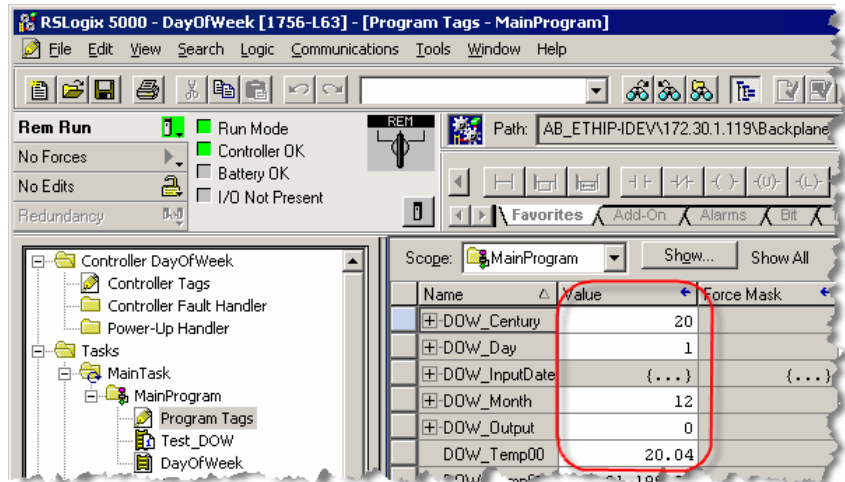
- c. Click the plus sign (+) next to **RSLogix 5000** to display the available actions.

- d. Select the **Allow** check boxes for **Controller: Clear Fault**, **Controller: Lock/Unlock**, **Firmware: Update**, and **Print: Report**. Also select the **Allow** check boxes for **Project Open** and **Project Go On-line**. These two are required. As a result, PSmith can perform the actions a shift leader might be expected to perform, like clear faults at the controller level, but all other actions are unavailable.

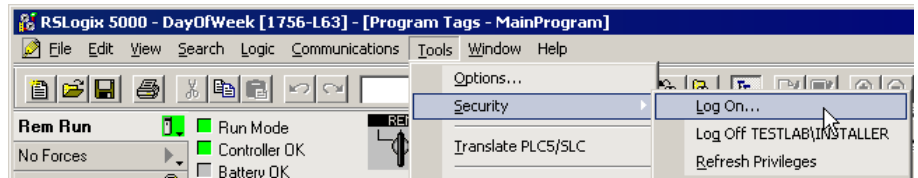


- e. Click **OK** to save the changes and close the dialog box.
6. Test the new security settings in Logix Designer application:

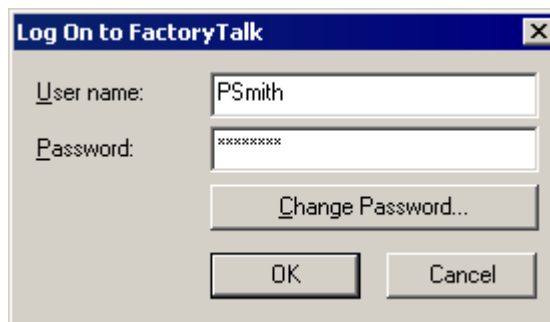
In the Controller Organizer, expand **Tasks > Main Task > Main Program** and then double-click **Program Tags**. Notice that the currently logged on FactoryTalk user (you should be logged in as a user with administrative rights) is able to edit tag values.



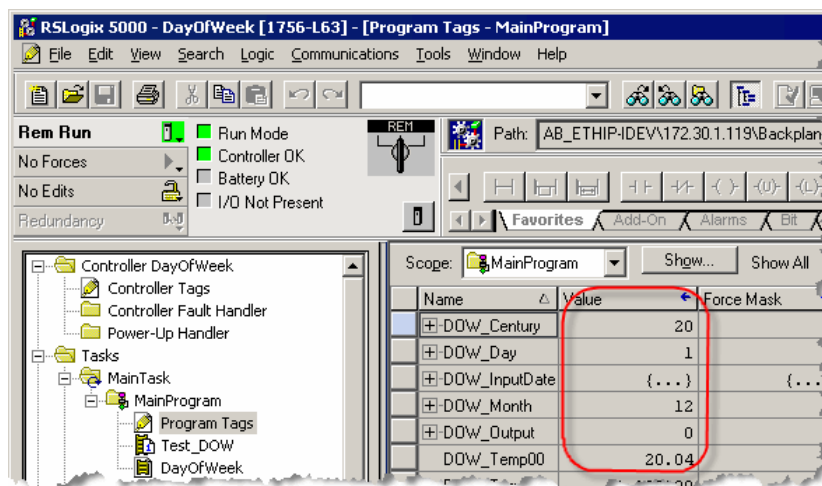
7. Now log on to FactoryTalk as PSmith:
 - a. From the **Tools** menu, select **Security > Log On**.



- b. In the **Log On to FactoryTalk** dialog box, enter the user name **PSmith**, enter **password** for the password, and then click **OK**.



- c. Now look at the Program Tags. Notice that PSMith is not able to edit tag values.



PSmith is allowed to view the tags and programs, but is not allowed to make any changes.

8. Log on again as a user with administrative rights if you want to make additional security changes.

Securing PLCs

You can use RSLogix 5 or RSLogix 500 software to program PLC controllers. To set up FactoryTalk security for these controllers, you need to work in RSLogix 5 or RSLogix 500 software (depending on the type of PLCs you have) and FactoryTalk. For details refer to the user documentation and online help for RSLogix 5 or RSLogix 500 software.

PLCs use both logical names and network relative paths. Use either logical names or network relative paths, or you can have a mix of both.

Permission sets and logical names

Permission sets and Logical Names identify a set of actions that are allowed or denied for one or more user groups or computer groups. You use permission sets and Logical Names to define user permissions in the FactoryTalk Administration Console. Use permission sets to apply the same permissions to multiple controllers or project components. Use a Logical Name to associate permissions with a specific controller. When you use a Logical Name, it must match the name of the controller.

When a user opens a project that has been secured with a permission set or a Logical Name and configured to use only the selected security authority, the Logix Designer application checks the ID of the FactoryTalk Directory to see if it matches the ID stored in the project.

- If the ID matches, the Logix Designer application checks the directory and finds the Logical Name (that matches the controller name), or the permission set associated with the project, and gets the permissions for the current user/computer combination.

- If the ID does not match, the project uses the Guest User permissions defined for that permission set or Logical Name.

When a user opens a project that has been secured but has **not** been configured to use only the selected security authority, the Logix Designer application checks the connected FactoryTalk Directory, finds the Logical Name or the permission set associated with the project, and gets the permissions for the current user/computer combination. Rockwell recommends configuring the project to use only the selected security authority to maintain control over the directory that secures the project.

Permissions for Guest Users

When you configure permission sets and logical names in the FactoryTalk Administration Console, you can also configure permissions for Guest Users. The permissions for Guest Users determine the level of access for users who are not authenticated on the same FactoryTalk directory that the project was secured with.

Permissions for Guest Users are cached in the project file to which they are associated. However, the permissions are only stored in the project file for permission sets that have been applied to objects by a user of the primary FactoryTalk directory.

Refer to the FactoryTalk online help for more information on permissions for Guest Users.

Where to go from here

Do one of the following:

- Continue assigning security permissions for RSLogix 5000, if desired.
- Go to [RSLinx and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLinx software.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components
- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.
- Go to Chapter "Configure Source Protection in Logix Designer Application" of Logix5000 Controllers Security Programming Manual for information on using the application Source Protection utility to secure your Logix Designer application routines.
- Refer to the Logix CPU Security Tool v3.0 User Manual located on the Studio 5000 CD in the */Tools* directory. The tool itself is also available

on the Studio 5000 CD in the */Tools* directory and from the Support web site downloads at www.software.rockwell.com/support/download/.

Use the following search criteria:

Category: **Downloads**

Sub-Category: **Utilities**

Product: **RSLogix**

FactoryTalk View SE and FactoryTalk Security

FactoryTalk Security manages security for FactoryTalk Directory itself, the application, the areas (and their contents) within the application, and participating users, computers, and devices. For network applications, this includes information about which computers users are allowed to access.

In FactoryTalk View Studio, you can specify the levels of access that users or groups of users have to each of these resources when they develop and run applications. Do this by allowing or denying permission to perform certain actions on a resource.

FactoryTalk View security manages run-time security for HMI project components, including FactoryTalk View commands and macros, graphic displays, OLE objects, and HMI tags.

Before you begin

- Verify that you have installed and activated the software listed below under [What you need](#) on [page 151](#).
- FactoryTalk View (CPR 9 or later) installation disc
- Become familiar with the terms and concepts of FactoryTalk Security. See [Understanding automation security](#) on [page 17](#) and [About the FactoryTalk system](#) on [page 21](#) for more information.

What you need

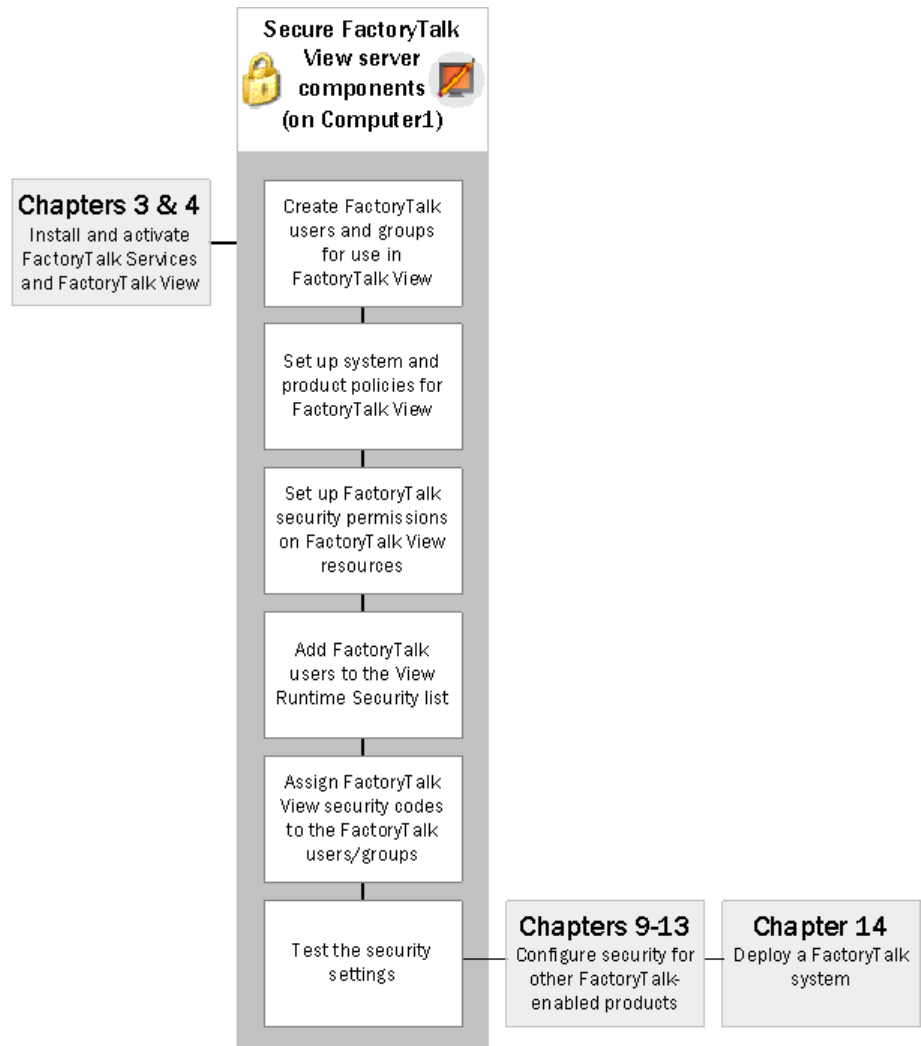
On the computer acting as the FactoryTalk View SE server (**Computer1** in our sample scenario):

- FactoryTalk Services Platform v. 2.10 (CPR 9) or later. Using the newest available version is recommended.
- FactoryTalk Activation
- FactoryTalk View SE Server components (including the sample applications)
- Microsoft® Internet Information Server
- RSI Utilities
- RSLinx Enterprise or RSLinx Classic

On the computer acting as the FactoryTalk View SE client (**Computer2** in our sample scenario):

- FactoryTalk Services Platform v. 2.10 (CPR 9) or later. Using the newest available version is recommended.
- Microsoft® Internet Information Server
- FactoryTalk Activation
- FactoryTalk View SE client components (including FactoryTalk View Studio, View Editors, and the sample applications)
- RSI Utilities

Follow these steps



Creating FactoryTalk Security accounts

Before you can add users and user groups to FactoryTalk View SE User Accounts, you first have to create accounts for them in FactoryTalk Security services. It is recommended that you create FactoryTalk Security user group accounts and set up security permissions to resources for them first, then you can create user accounts and assign them to the appropriate user group.

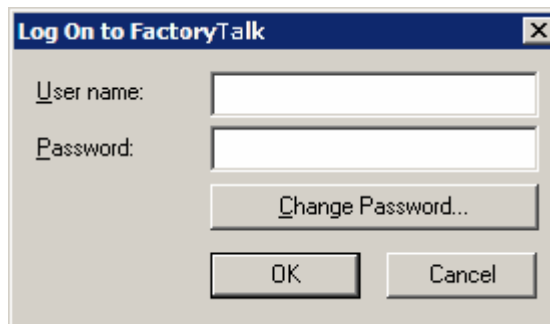
All users within a particular group inherit the security permissions set up for the group. This makes it easier to assign and manage permissions for

multiple users with similar security needs. If you change any of the permissions for the group, all members inherit the changes.

For detailed information about creating users and user groups in FactoryTalk Security, see the FactoryTalk Security Help.

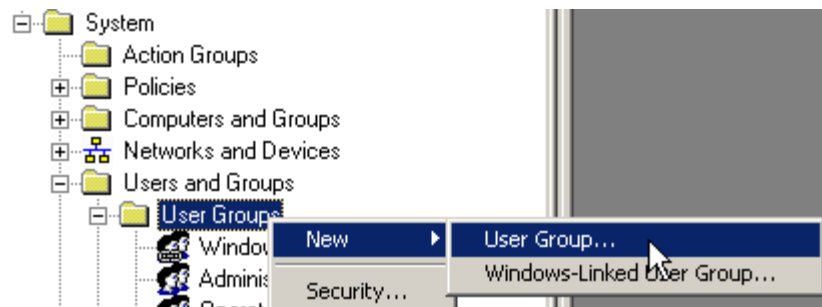
On Computer1 (where FactoryTalk Administration Console is installed):

1. Create a user group account in FactoryTalk Security:
 - Open FactoryTalk Administration Console from **Start > Rockwell Software > FactoryTalk Administration Console**.
 - If prompted to log on to FactoryTalk, enter a valid FactoryTalk user name and password, and then click **OK**.

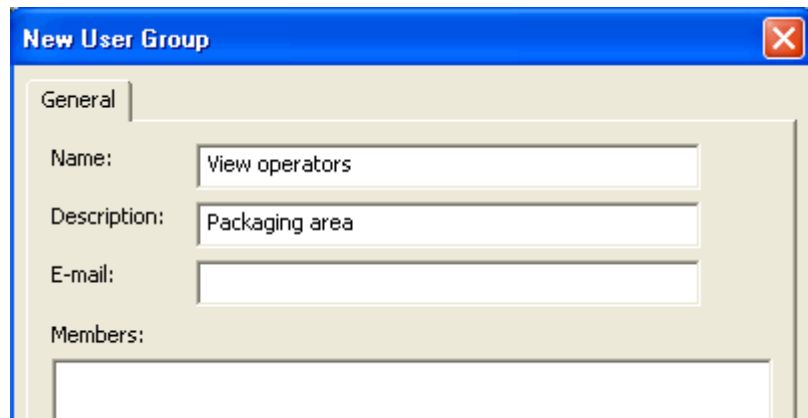


Tip: In FactoryTalk Security CPR 9 or later, single sign-on is enabled by default, so users are not prompted to log on to FactoryTalk. If you are upgrading from CPR 7, or if you changed the default FactoryTalk security configuration, you will be prompted to log on.

- In the Explorer window, open the **Users and Groups** subfolder in the **System** folder.
- Right-click the **User Groups** folder, and select **New > User Group**.

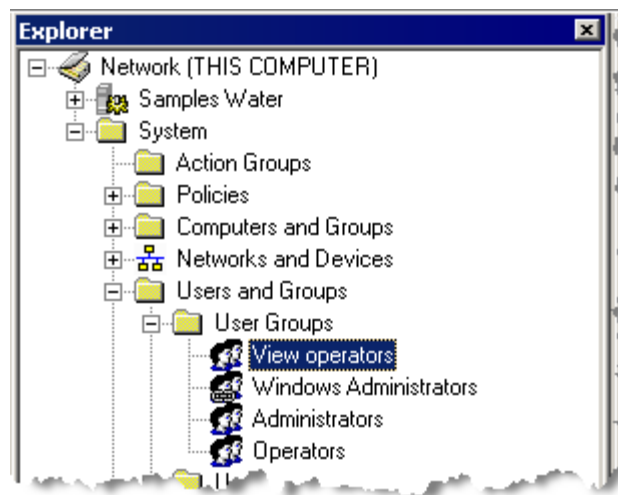


2. Type a **Name** and **Descriptor** (use the information shown below for this example).



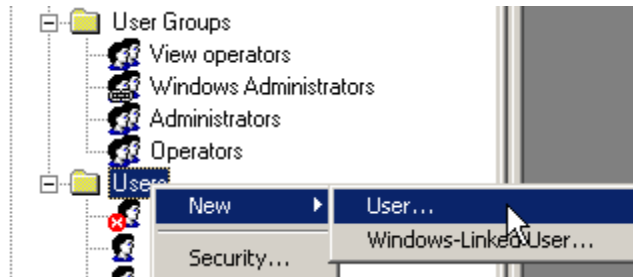
Tip: If you have an existing Windows user group, you can add a security account for it by selecting **Windows-linked User Group**.

3. Click **Create** to create the security account for the user group and close the dialog box. When you click the **User Groups** folder to open it, you will see the user group you have just added.



4. Create a new user account in FactoryTalk Security:

- In the Explorer window, open the **Users and Groups** subfolder in the System folder.
- Right-click the **Users** folder, and select **New > User**.



Tip: You can add existing Windows users by selecting **Windows-linked User**.

- In the **General** tab of the **New User** dialog box, specify the user's login name and password, and other information, as necessary.

For details about the options in the dialog box, click the **Help** button.



For this example, enter the following:

User name: **BJones**

Full name: **Bob Jones**

Description: **View operator**

Password: **password**

For this example, clear the **User must change password at next logon** check box, and then select the **Password never expires** check box.

- Click **Create** to add a security account for the user. The new user appears in the Users folder.



5. Add user accounts to the user group in FactoryTalk Security:

- In the Explorer window, open the **Users and Groups** subfolder in the System folder.
- Double-click the **User Groups** folder, right-click the user group you created in step 2 (our example used **View operators**), and then select **Properties** from the pop-up menu.
- In the **General** tab of the **Group Properties** dialog box, click the **Add** button.
- In the **Select User or Group** dialog box, select the **Show users only** option to display the list of available users.
- Select the user you wish to add to the group (our example was **BJones**), and click **OK**.

For details about the options in the dialog box, click the **Help** button.

- Click **Ok** to close the **Group Properties** dialog box.

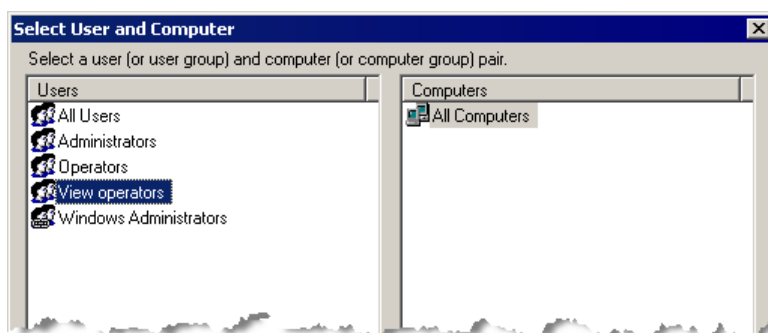
6. Specify actions that users can perform on a resource:

To secure access to a system resource, specify which users or groups of users have permission to perform actions on the resource.

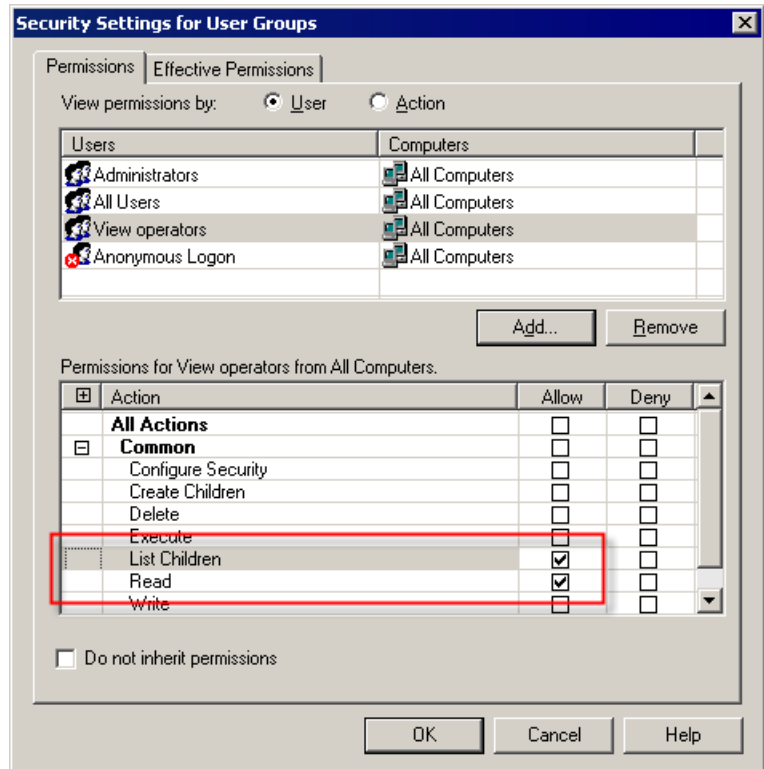
- In the Explorer window, open the **Users and Groups** subfolder in the System folder.
- Right-click the **User Groups** folder, and then select **Security** from the pop-up menu.



- In the 'View permissions by' section of the **Security Settings for User Groups** dialog box, click the **Add** button.



- For this example, select **View operators**, and then click **OK**. The View operators group is added to the list.
- Expand the list of Common actions by clicking the plus sign (+) in the left column.

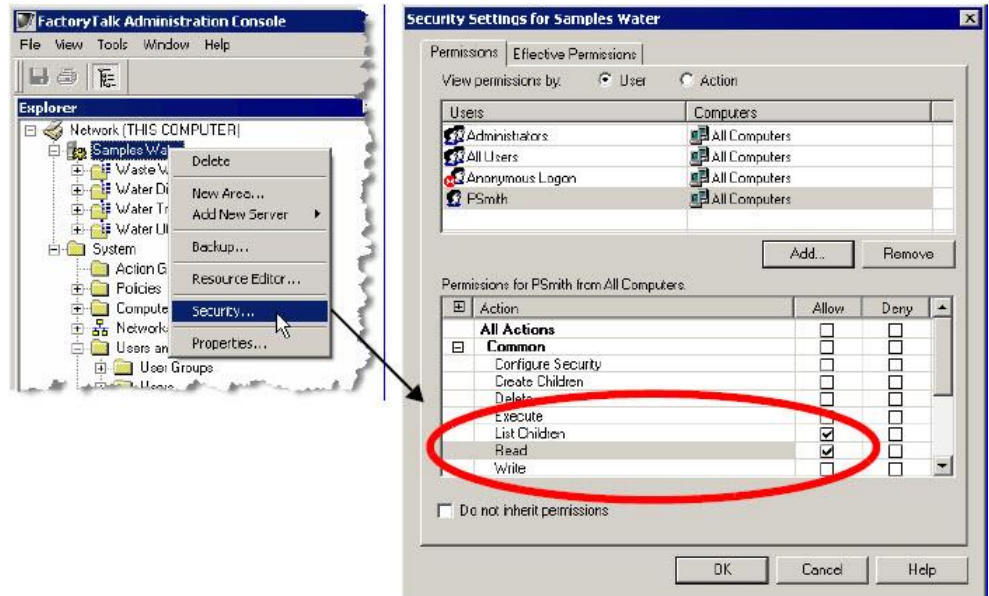


- As shown in the above illustration of the **Security Settings** dialog box, select the check boxes next to **List Children** and **Read**.

This gives the **View operators** group permission to perform the Common actions *Read* and *List Children* on the FactoryTalk Network Directory. This means that members of the group are able to run the FactoryTalk View SE client.

- Click **OK** to save the settings and close the dialog box.

Tip: FactoryTalk View SE users must have Read and List Children rights at the application level. The easiest way to do this is at the root of the FactoryTalk Directory tree.



Set up system and product policies

In both FactoryTalk Administration Console and FactoryTalk View Studio you can set up product and system policies that determine general characteristics of the system.

Example: This security configuration guide uses the default FactoryTalk Security settings for FactoryTalk View SE system and product policies, therefore we will not discuss the actual procedures for changing those defaults. The following sections are intended as an overview. For detailed information, refer to the FactoryTalk Security Help and to Chapter 5 in the *FactoryTalk View Site Edition User's Guide, Volume 1*.

These specifications are stored at the FactoryTalk Directory and, like all settings in the System folder, apply to all FactoryTalk products managed by a single Local Directory or Network Directory.

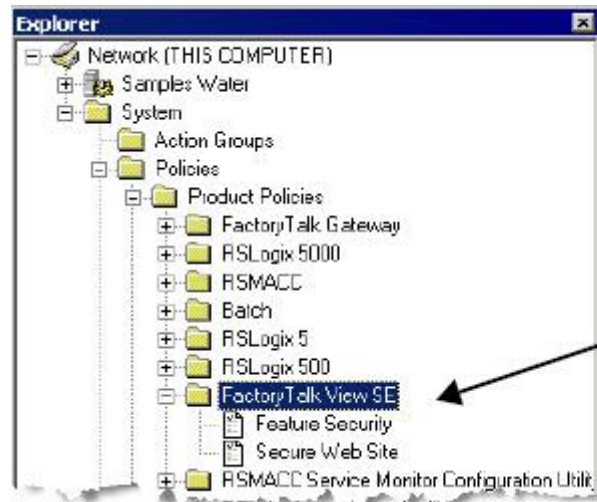
The following illustration shows you where to find the Policies folder in the Explorer window:



Product policies

Product policies are sets of features that you can secure for the individual products in a FactoryTalk system.

The following illustration show a list of the FactoryTalk View SE product policies.

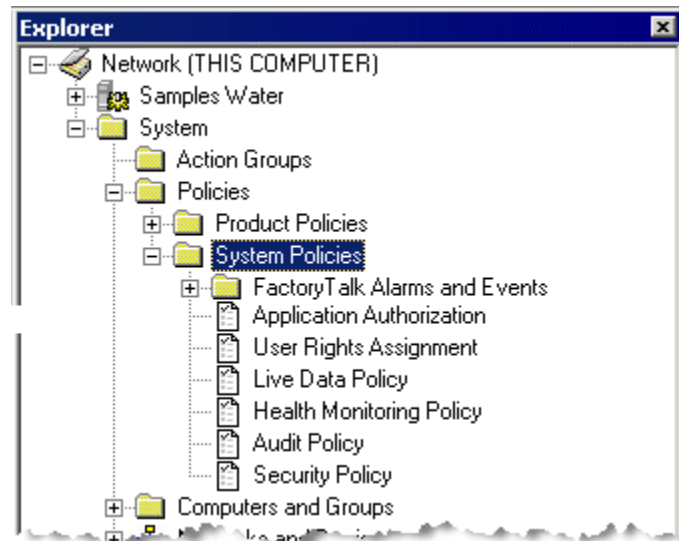


For FactoryTalk View SE, you can set up product policies for configuring and using secure web sites under Internet Information

Only users with the required level of access can use the product features that you have secured. For details about setting up product policies, see the FactoryTalk Security Help. For more information on configuring and using secure web sites under Internet Information Services, click **Help** in the FactoryTalk View SE Secure Web Site Setup tool.

System policies

In a FactoryTalk View SE application, you can set up the following system policies:



- **FactoryTalk Alarms and Events** policies, which determine the system-wide behavior of alarms and events.
- **Application authorization** policies allow you to authorize applications that have access to FactoryTalk Directory and to configure whether to verify the application publisher information.

Important: Some applications of Microsoft (for example, msexec.exe) are not signed. Some earlier versions of FactoryTalk products were not signed when they were released. You may fail to verify the publisher information on these applications. For more information about versions of FactoryTalk products signed, see FactoryTalk Security Help.

- **User rights assignment** settings determine which users can backup and restore FactoryTalk Directory contents, change the directory server, manually switch the Active and Standby servers in a redundant server pair, or modify the security authority identifier.
- **Health monitoring policy** settings define system availability parameters. These include how often the system checks network connections to remote computers, and how long a network disruption can last before the system determines that communications have failed.



Changing health monitoring policy settings can result in unexpected behavior. For most networks, the default policy settings provide the best results.

- **Live Data policy** settings determine which communications protocol will be used in a FactoryTalk system distributed over a network.



Changing live data policy settings can result in unexpected behavior. Do not change the settings in a running production system. For changes to take effect, all computers on the network must be shut down and restarted.

- **Audit policy** settings determine what security information is recorded while the system is in use. This includes whether FactoryTalk Diagnostics logs an audit message when a user attempts an action and is allowed or denied access.
- **Security policy** settings determine general characteristics of security accounts and passwords. This includes whether single sign-on is enabled, and how many invalid logon attempts are allowed before an account is locked out.

For more details about setting up system policies, see FactoryTalk Security Help.

Add FactoryTalk user accounts to FactoryTalk View

After you have created users and groups in FactoryTalk Security, you add them to the security accounts list in the Runtime Security editor in FactoryTalk View SE. When you add an account, you also assign the security codes that will give those users and user groups access to secured HMI components. (Secured HMI components are those that have been assigned security codes.) These codes (A through P), along with those assigned to HMI project components, determine which components a user has access to at run time.

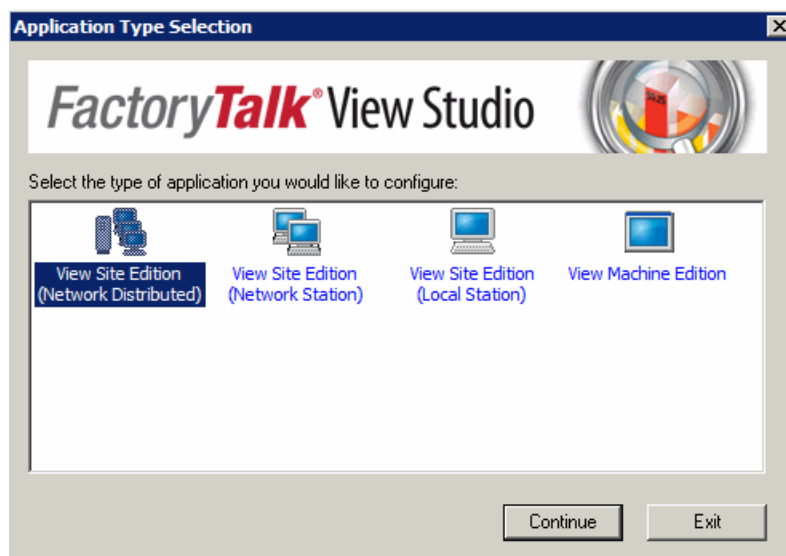
To restrict access to a command, macro, graphic display, OLE object verb, or HMI tag, you assign a security code from A through P to it, and then assign that code only to the users who are supposed to have access to the component.

For more information about how these features are used in FactoryTalk View, and for examples of assigning FactoryTalk Security permissions to FactoryTalk View users and user groups, see Chapter 5 in the *FactoryTalk View Site Edition User's Guide, Volume 1*.

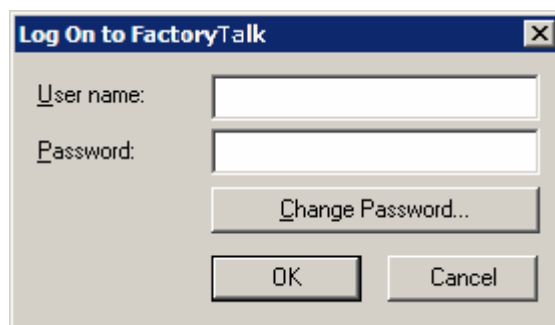
On Computer2 (where FactoryTalk View Studio is installed):

1. Open FactoryTalk View Studio:

- Select **View Site Edition (Network Distributed)** and click **Continue**.

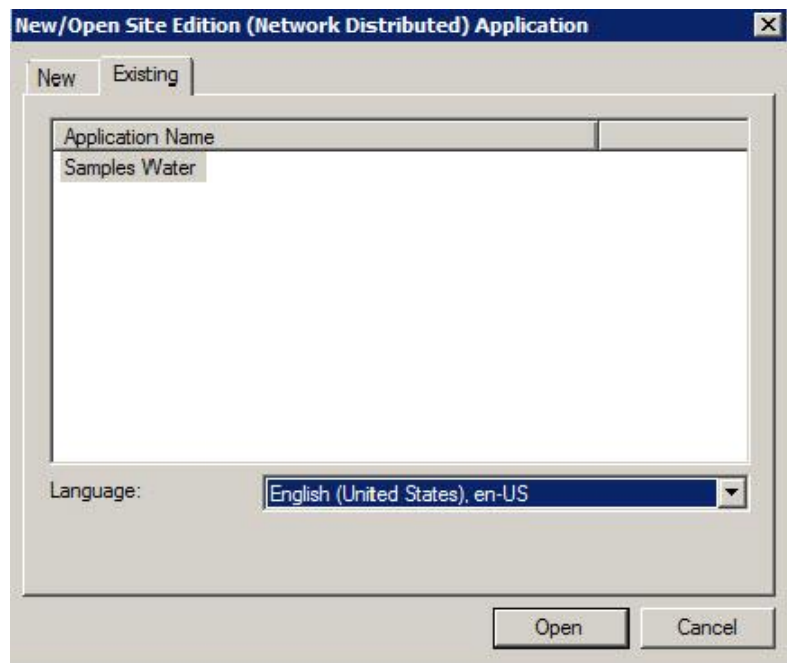


- If prompted to log on to FactoryTalk, enter a valid FactoryTalk **administrator** user name and password, and then click **OK**.



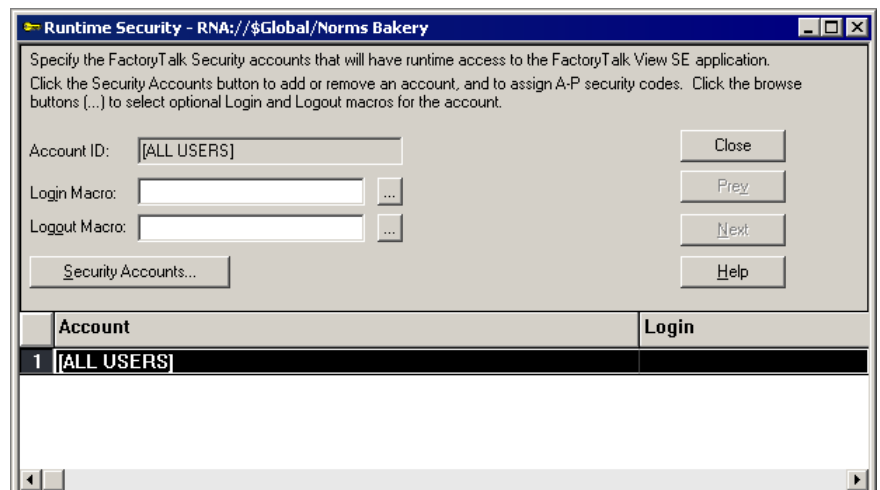
Tip: In FactoryTalk Security CPR 9 or later, single sign-on is enabled by default, so users are not prompted to log on to FactoryTalk. If you are upgrading from CPR 7, or if you changed the default FactoryTalk security configuration, you will be prompted to log on.

- On the **New/Open Site Edition (Network Distributed) Application** dialog box, click the **Existing** tab, and then select **Samples Water** from the application list.
- Select **English (United States), en-US** for the default language (if not already selected) and then click **Open**.

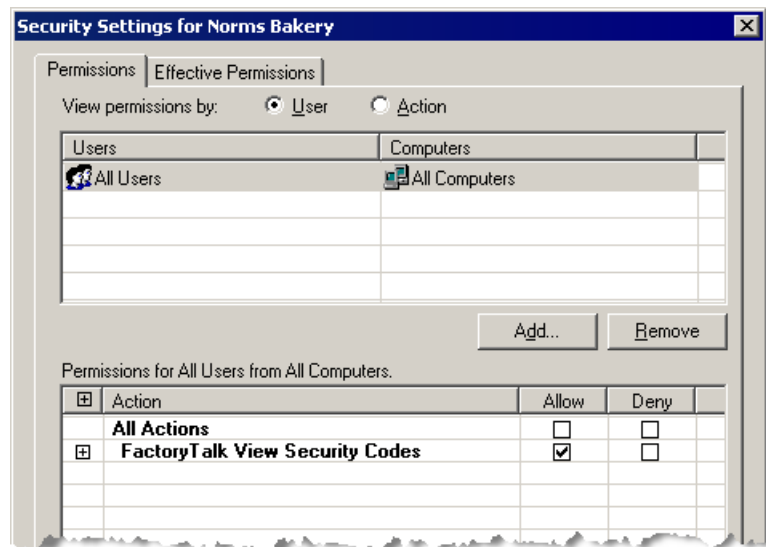


2. Open the Runtime Security editor:

- In FactoryTalk View Studio, select **Runtime Security** from the **Settings** menu.



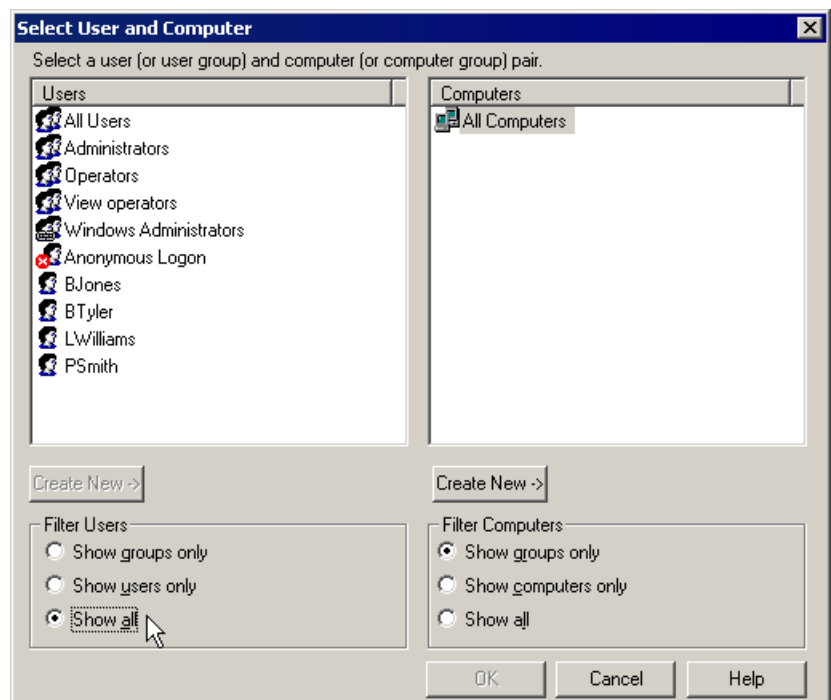
- In the **Runtime Security** editor, click the **Security Accounts** button to open the **Security Settings** dialog box.



Tip: If you want to tighten security completely, select **All Users** and then click the **Remove** button. Then add in only those users and groups you want to have access.

3. Add FactoryTalk users to your View applications:

- In the **Security Settings for [Application Name]** dialog box (this example uses Norms Bakery), click the **Add** button to open the **Security** dialog box.

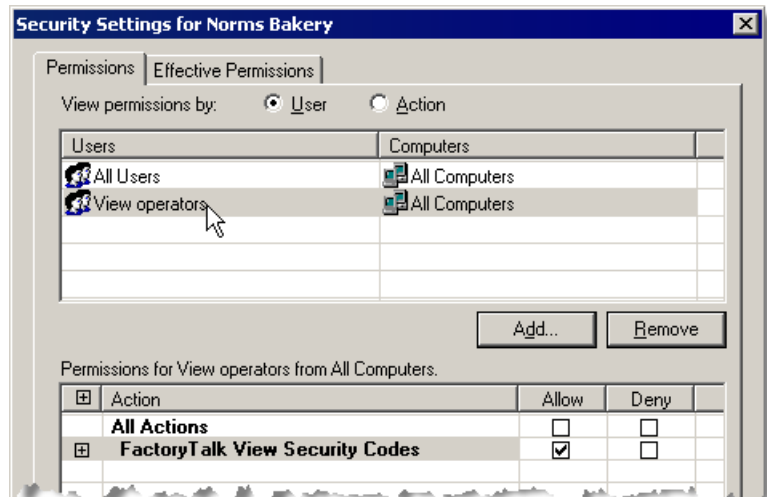


- In the **Select User and Computer** dialog box, click the name of a user or group to be added to the Runtime Security user accounts list, and then click **OK**. For this example, select **View operators**.

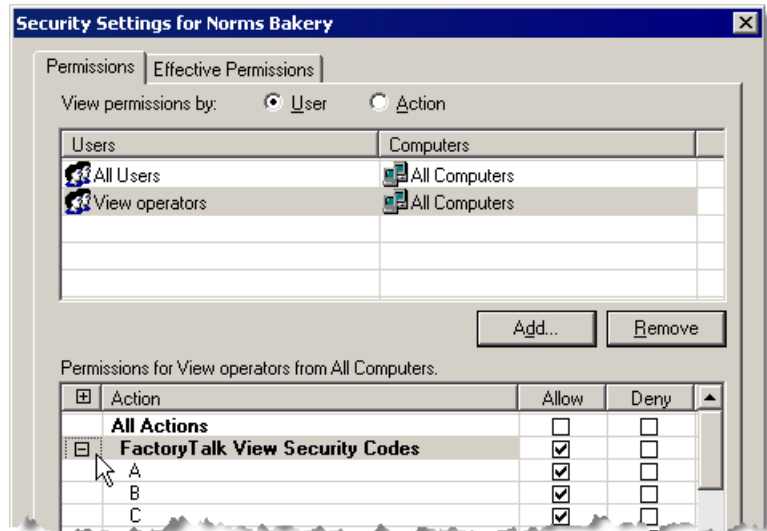
For a network distributed application or network station application you can click **Show all** in the Filter Computers frame if you are going to assign a specific computer (or computer group) to the user. The default is for the **All Computers** option in the Computers list to be selected.

Tip: If you are setting up security for a network distributed application or network station application, you must select a computer account with the user account before you can click **OK**. If there is only one computer on the list it is selected by default.

- In the **Permissions** tab of the **Security Settings** dialog box, ensure that the user or group you have just added is selected in the ‘View permissions by’ section of the tab.



- Expand the FactoryTalk View Security Codes by clicking the plus sign (+) in the left column.



- For this example, clear the check box next to **FactoryTalk View Security Codes**, then select **A**, **B**, and **C** by selecting the **Allow** check box beside each code.

Any user in the View operators group on Computer2 now has run-time access only to those commands that have an A, B, or C security code assigned.

- Click **OK**.

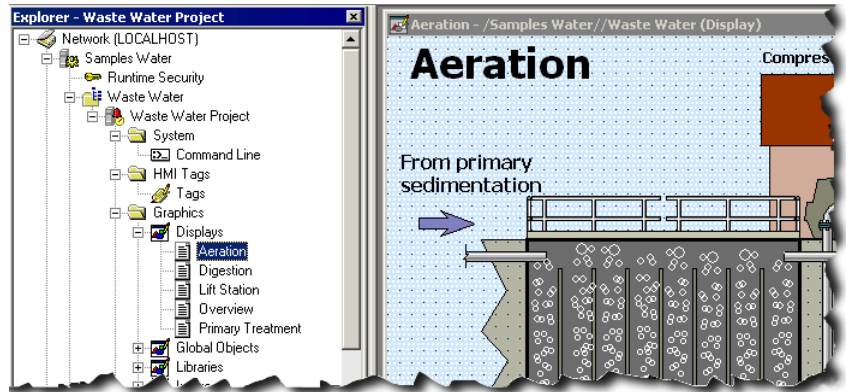
In the **Runtime Security** dialog box, you can also specify login and logout macros for the user or group you have just added, if desired.

Important: Be sure to add the Administrators group (or a user with administrative rights) to the Runtime Security editor so that you will be able to make changes to and exit View Studio. Allow that group or user access to all security codes (select the **Allow** check box for **FactoryTalk View Security Codes**).

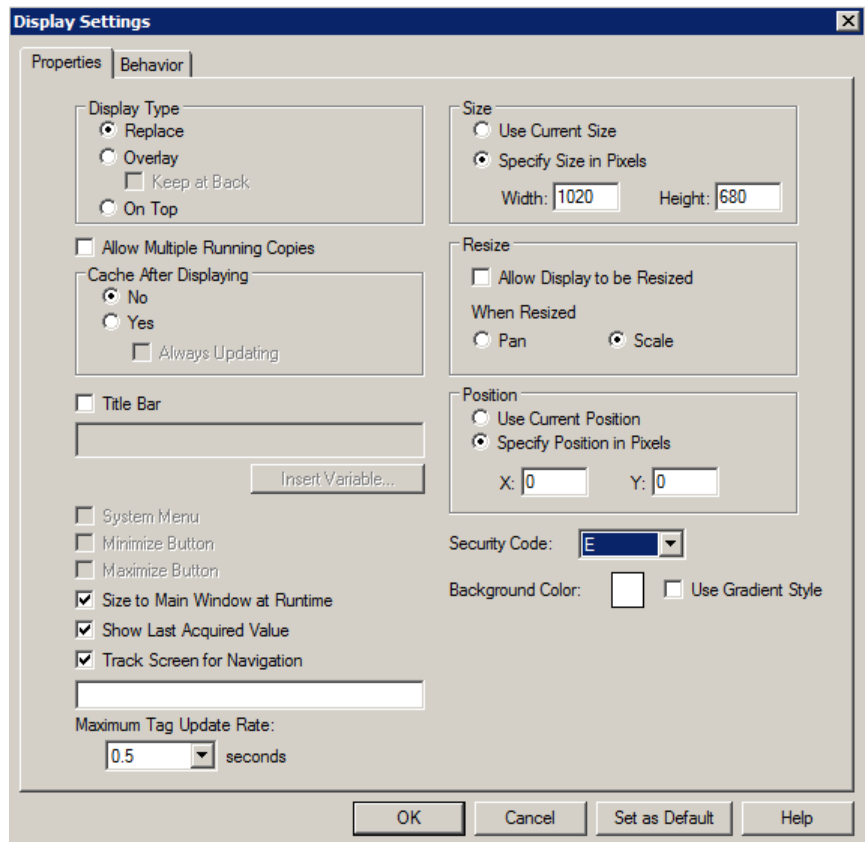
- Click the **Close** button to close the **Runtime Security** dialog box. Click **Yes** to save the application.

- Set FactoryTalk View security on an object:

- In the Explorer window, expand **Graphics > Displays** and double-click **Aeration** to open it.

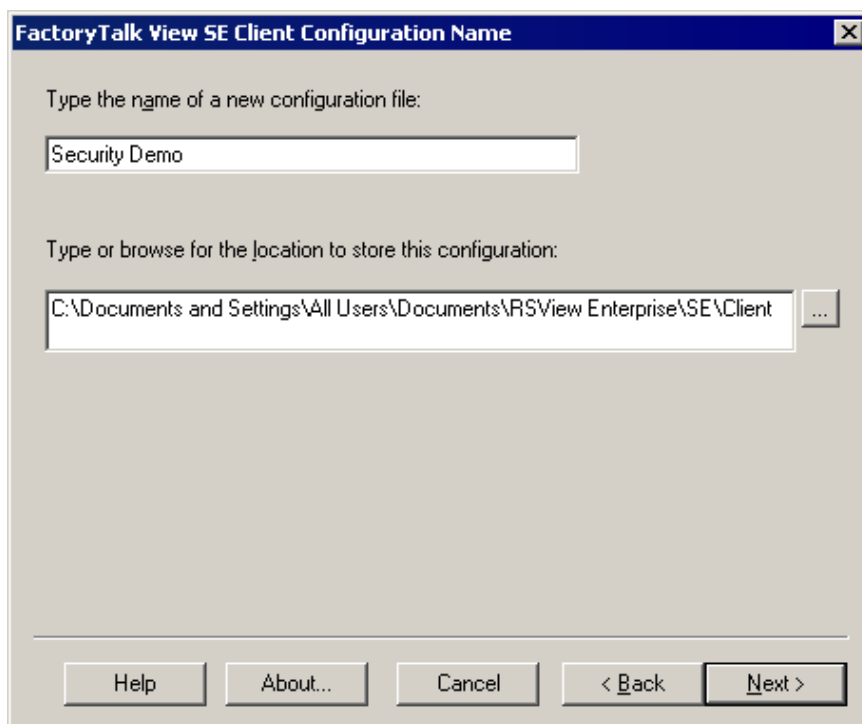


- From the **Edit** menu, select **Display Settings**. The **Display Settings** dialog box opens.

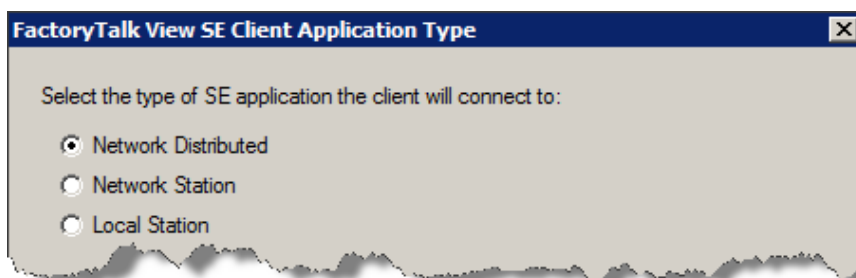


- From the **Security Code** drop-down list, select **E** (or a code that you have not assigned to one of the FactoryTalk users or groups), and then click **OK** to save the change and close the dialog box.
 - Save the application by selecting **Save** from the **Edit** menu.
1. Create a sample application:

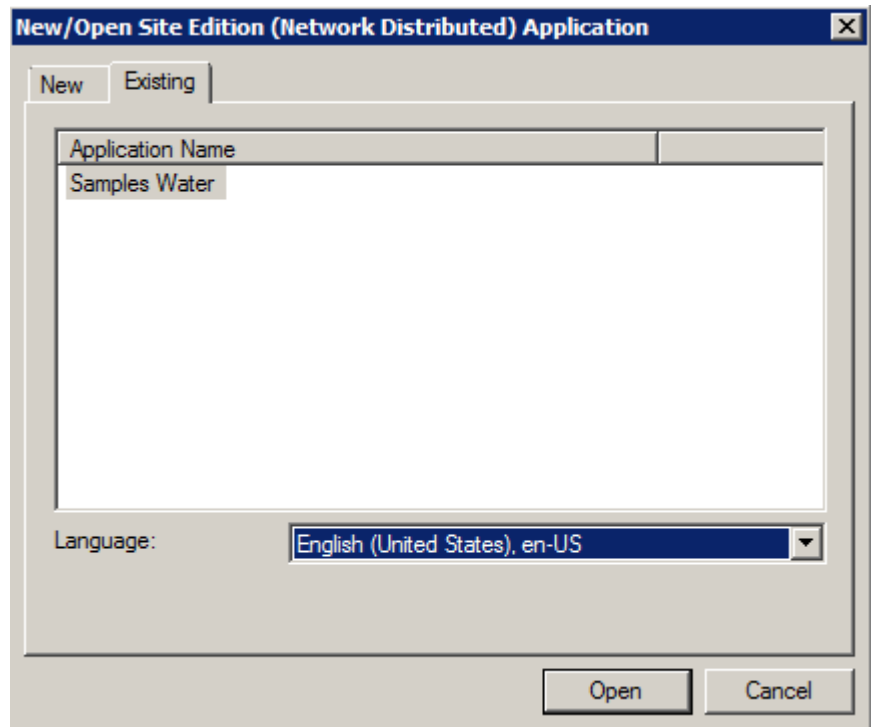
- Log on as a user with administrative rights.
- Click the **Launch SE Client** button  on the toolbar and then click **New** twice.
- In the **Configuration Name** dialog box, type **Security Demo** as the name of the new configuration file. Leave the default location. Click **Next**.



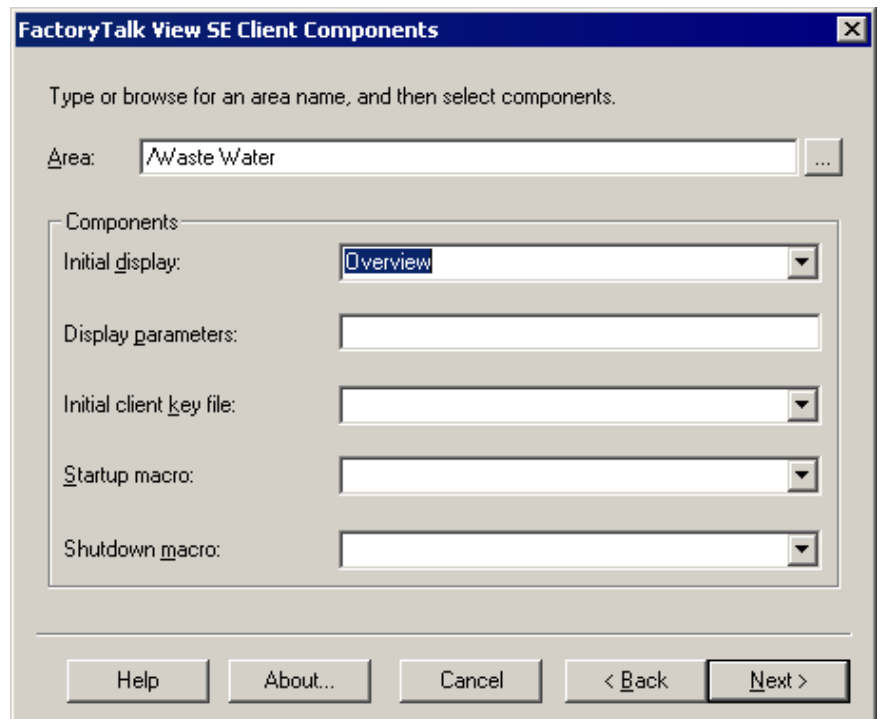
- Select **Network Distributed** as the application type and then click **Next**.



- On the **Application Name** dialog box, select **Samples Water** from the list of applications. Select **English (United States), en-US** as the default runtime language, and then click **Next**.



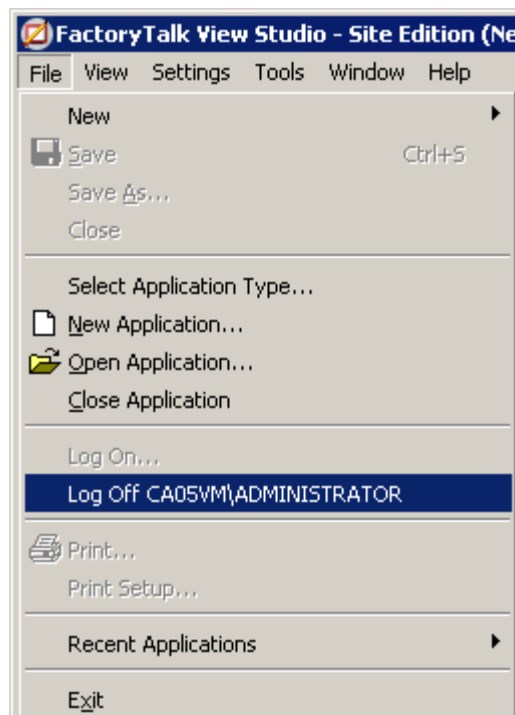
- On the **Client Components** dialog box, select **Waste Water** from the list of areas. Select **Overview** for the Initial display, and then click **Next**.



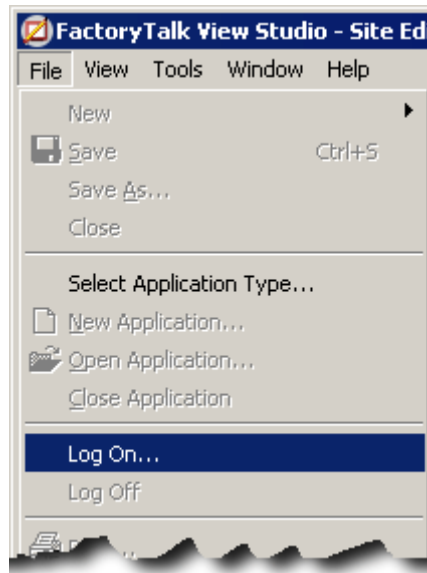
- Clear the **Show title bar** check box, and then click **Next**.
- Click **Next** again, and then click **Finish**. The Security Demo application loads and then opens to the Overview display:



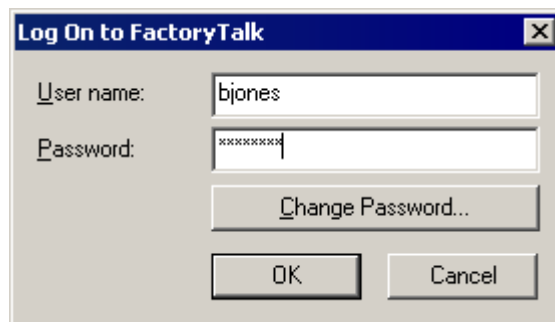
- Click the **Aeration** button. If you are logged in as an administrative user, the Aeration display opens.
 - Click the **Overview** button, and then click the **Close SE Client** button. Click **Yes** to confirm the exit command.
2. Now log off as the administrative user, log on as **Bob Jones**, and then run the Security Demo application:
- From FactoryTalk View Studio, select **Log Off** from the **File** menu.



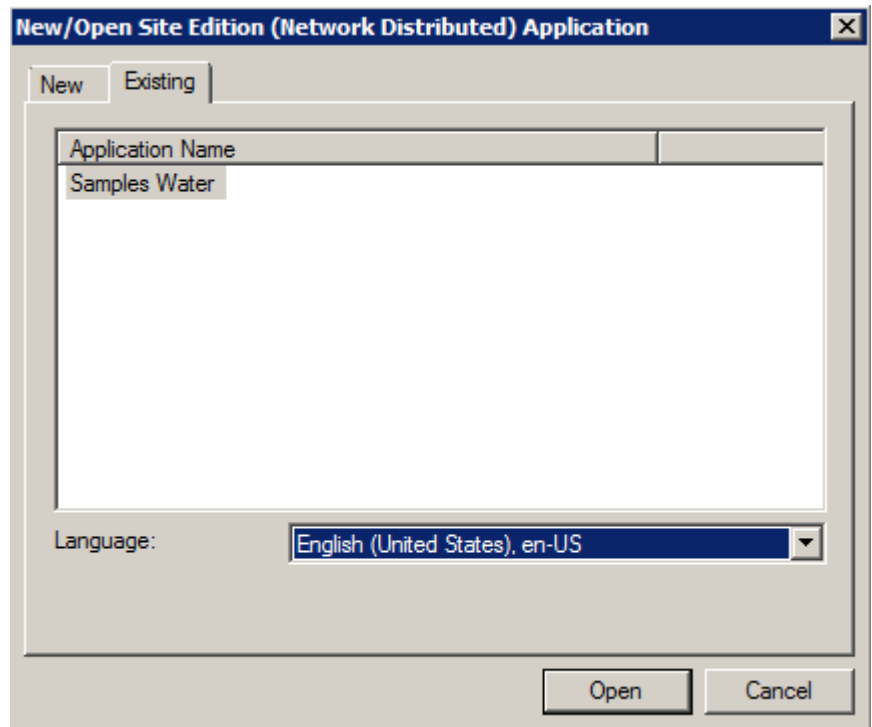
- Click **Yes** to close the application.
- To log on as Bob Jones, select **Log On** from the **File** menu.



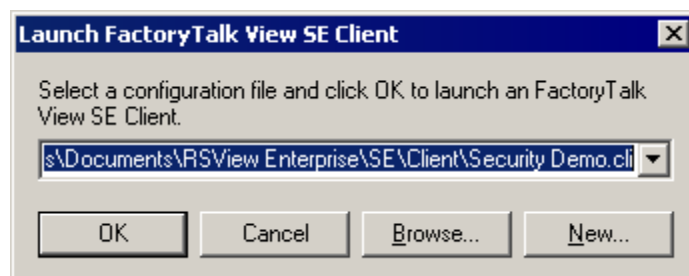
- Enter **BJones** as the User name, type **password** in the Password field, and then click **OK**.



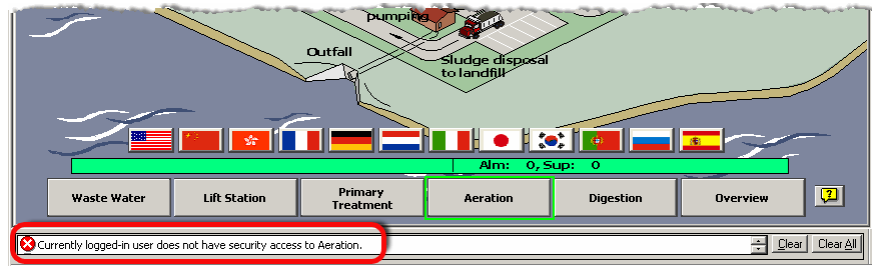
- In the **New/Open Site Edition (Network Distributed) Application** dialog box, select the **Samples Water** application, select **English** as the default language, and then click **OK**.



- Click the **Launch SE Client** button (shown at left). If prompted to log in, log in as **BJones** with a password of **password**.
- From the **Launch FactoryTalk View SE Client** dialog box, select **Security Demo.cli**, and then click **OK**.



The application opens to the Overview display. Click the **Aeration** button and see what happens. Since you are logged on as Bob Jones (a member of the View operators group), who only has 'E' security access, nothing happens because the Aeration display requires A, B, or C security access. Notice the error message in the status bar: "Currently logged in user does not have security access to Aeration."



- Click the **Overview** button, and then click the **Close SE Client** button to close the application. Click **Yes** to confirm the close.

Where to go from here

Now that you've set up security for FactoryTalk View, do one of the following:

- Log in as an administrative user and continue assigning permissions for FactoryTalk View commands, graphic displays, and HMI tags, if desired.
- Go to [RSLink and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLink software.
- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure projects.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components
- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.
- Refer to the FactoryTalk View user documentation for additional methods of securing HMI projects, tags and graphics, using electronic signature verification, and locking users into the FactoryTalk View SE Client environment.

FactoryTalk View ME and FactoryTalk Security

FactoryTalk Security is a part of FactoryTalk Directory, which is installed with the FactoryTalk Services Platform. This means that security applies not only to the FactoryTalk View Machine Edition application, but to any other FactoryTalk-enabled software running on the same computer.

Instead of dealing with access to parts of the system, FactoryTalk Security is concerned first with authenticating users' identities, and then with verifying their authorization to perform specific actions within the system.

Important: For the CPR 9 version of FactoryTalk View ME, users are no longer associated with applications; they are associated with the FactoryTalk Directory. If you are deploying a FactoryTalk View ME application, be sure to back up and restore both the application and the FactoryTalk Directory or you will have to recreate the users on the runtime machine.

FactoryTalk Security allows you to reference user accounts that have already been set up in Windows. These are called *Windows-linked users*. The link symbol in the Explorer window indicates that a user is a Windows-linked user.

During the FactoryTalk View ME installation, the FactoryTalk Services Platform install grants the Windows Administrators and Authenticated User groups full rights to FactoryTalk security aware products.

The Windows-linked group called **Authenticated Users** is added to the FactoryTalk Network Directory and FactoryTalk Local Directory. This means that all users on any local computer that is connected to the Network Directory can access the Network Directory and all users on the local computer can access the Local Directory. By default, the desktop Windows user will be logged in when FactoryTalk View Studio opens, so FactoryTalk View Studio will not require a user to log on to FactoryTalk.



You can still create applications that include runtime security when running on FactoryTalk View ME Station. Windows CE supports FactoryTalk native users and groups. However, Authenticated Users are not supported on Windows CE platforms. On Windows CE terminals, Windows-linked users must be added to the FactoryTalk Directory before they can be logged in.

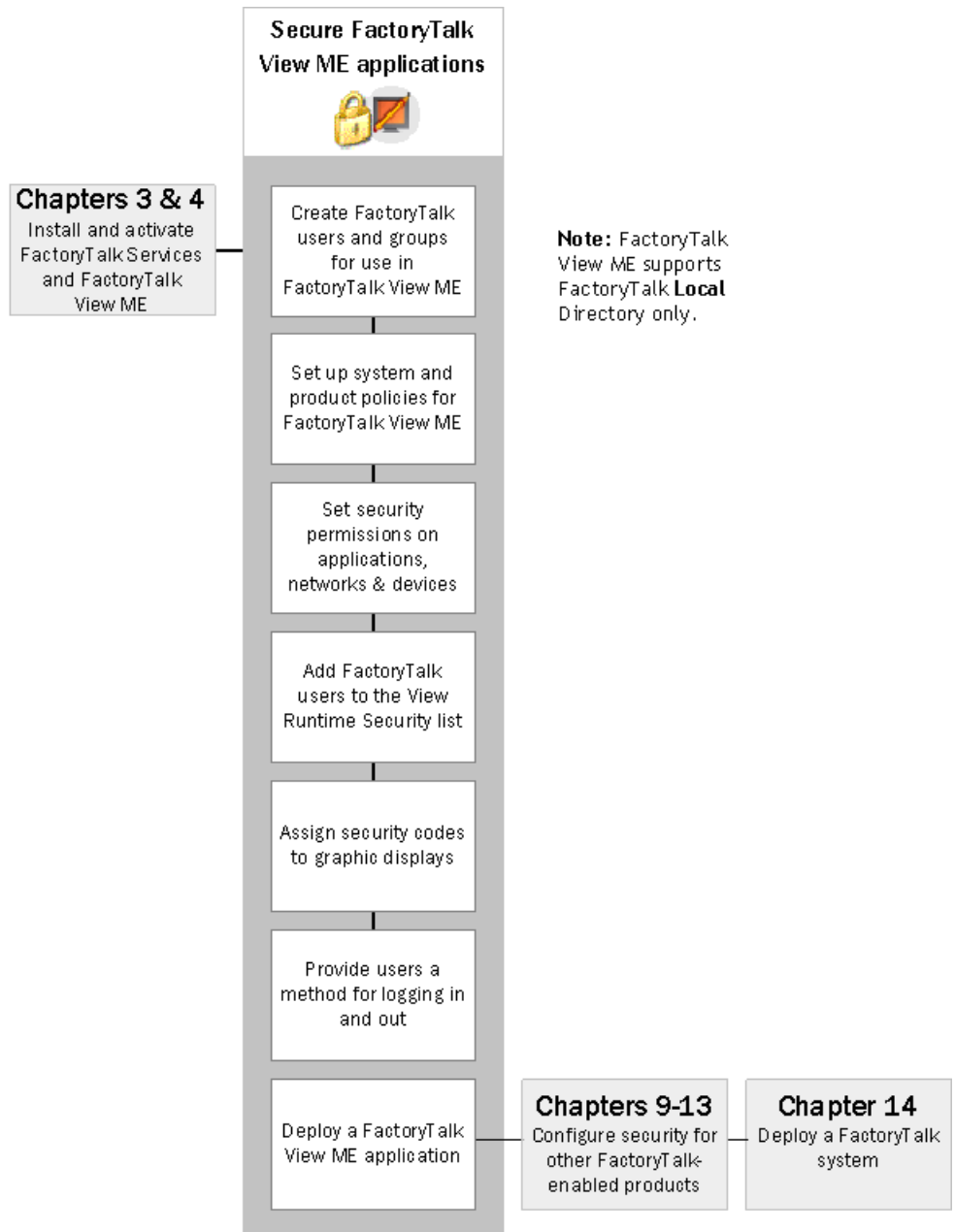
Before you begin

- Verify that you have installed and activated the software listed below under [What you need](#) on [page 176](#).
- FactoryTalk View (CPR 9 or later) installation disc
- Become familiar with the terms and concepts of FactoryTalk Security. See [Understanding automation security](#) on [page 17](#) and [About the FactoryTalk system](#) on [page 21](#) for more information.

What you need

- FactoryTalk Services Platform v. 2.10 (CPR 9) or later. Using the newest available version is recommended.
- FactoryTalk Activation
- FactoryTalk View ME components (including the sample applications)
- RSI Utilities
- RSLinx Enterprise or RSLinx Classic

Follow these steps



Creating FactoryTalk Security accounts

Before you can add users and user groups to a FactoryTalk View ME application, the user and users groups have to be added or created in FactoryTalk Security. It is recommended that you create FactoryTalk Security native user groups and setup security permissions for them. You can then populate the FactoryTalk native groups with FactoryTalk native user or Windows-linked users or Windows-linked user groups. For example, you could create user groups called Maintenance and Engineers and then add the appropriate users or user groups to those groups. This is called role-based security.

All users within a particular group inherit the security permissions set up for the group. This makes it easier to assign and manage permissions for

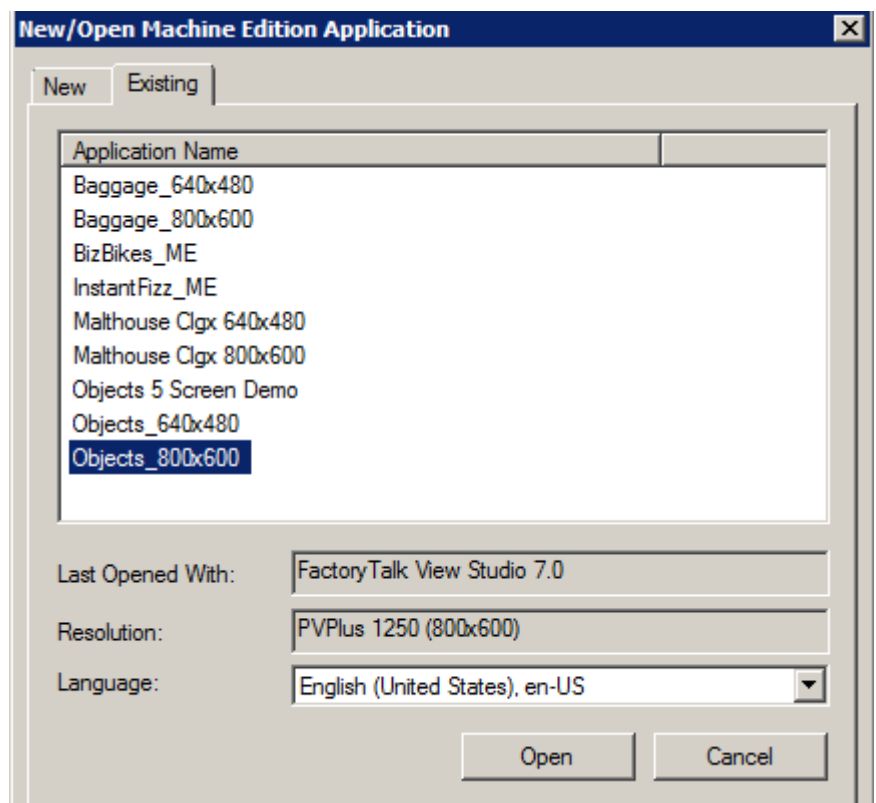
multiple users with similar security needs. If you change any of the permissions for the group, all members inherit the changes.

For detailed information about creating users and user groups in FactoryTalk Security, see the FactoryTalk Security Help.

Tip: Before creating a new application, back up the Local FactoryTalk Directory System folder as Default.bak. You will restore and use this default FactoryTalk Directory file each time you create a new application. This provides you a method to restore the default FactoryTalk Directory configuration before starting a new project.

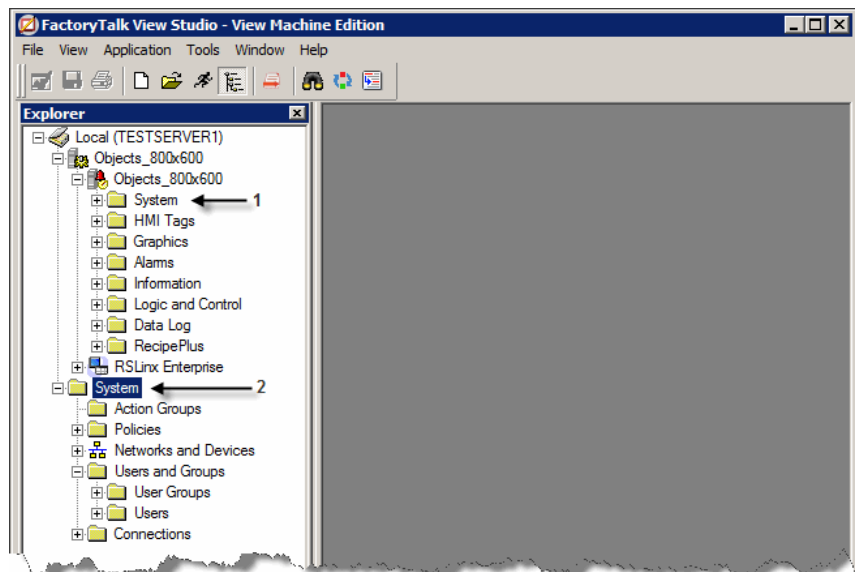
Add FactoryTalk user and group accounts

1. Launch FactoryTalk View Studio and open a FactoryTalk View ME application:
 - From the Windows **Start** menu, select **Rockwell Software > FactoryTalk View > FactoryTalk View Studio**.
 - Select **View Machine Edition** and then click **Continue**.
 - On the **Existing** tab, select the **Object_800x600** application, make sure the Language is **English**, and then click **Open**.



2. Add several users:

- In the FactoryTalk Directory **System** folder (marked with 2 below), expand the **Users and Groups** folder, right-click **Users**, and then click **New User**. For more information on the various System folders, refer to [About multiple System folders in FactoryTalk View](#) on [page 183](#).



The **New User** dialog box opens.

New User

General | Group Membership

User name:

Full name:

Description:

E-mail:

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Password:

Confirm:

- Specify the user name, password, and password options as follows:
User: **Eric**

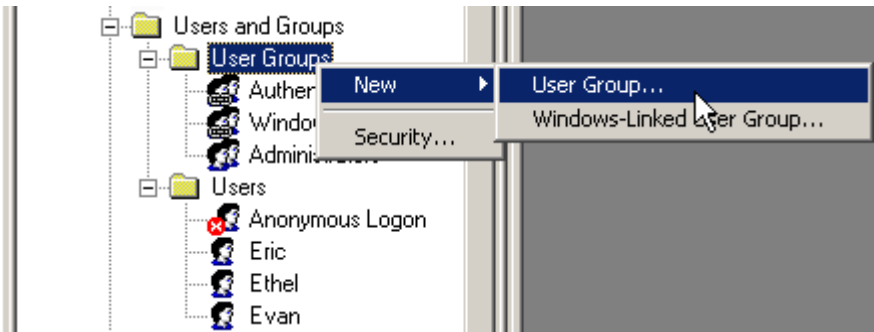
Password: **password**
Password never expires

- Click **Create**. The user is added to the Users folder as a native FactoryTalk user.
- Create two more users as follows:

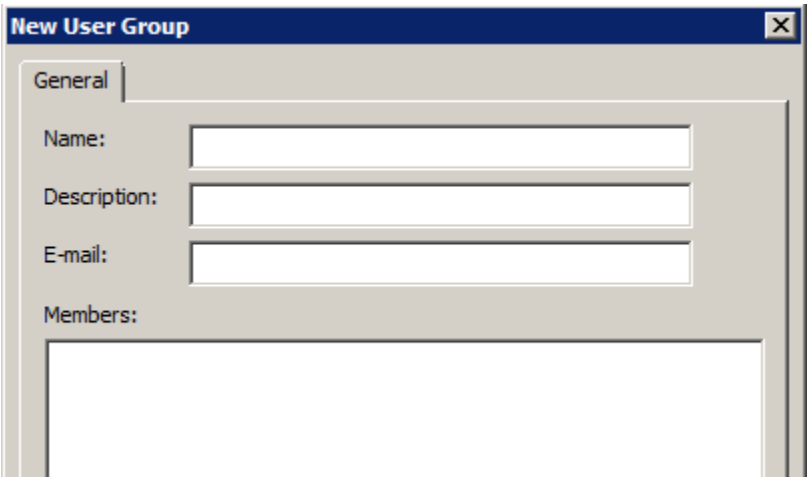
User: Evan	User: Ethel
Password: password	Password: password
Password never expires	Password never expires

3. Create a new User Group:

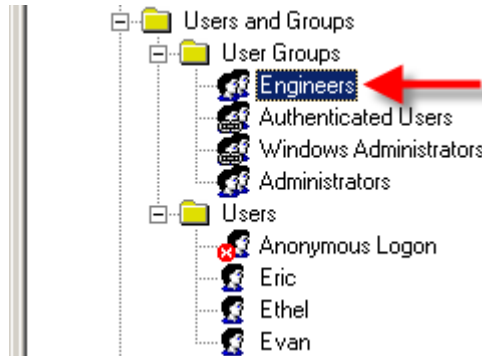
- Right-click **User Groups**, and then select **New > Group**.



The New User Group dialog box opens:

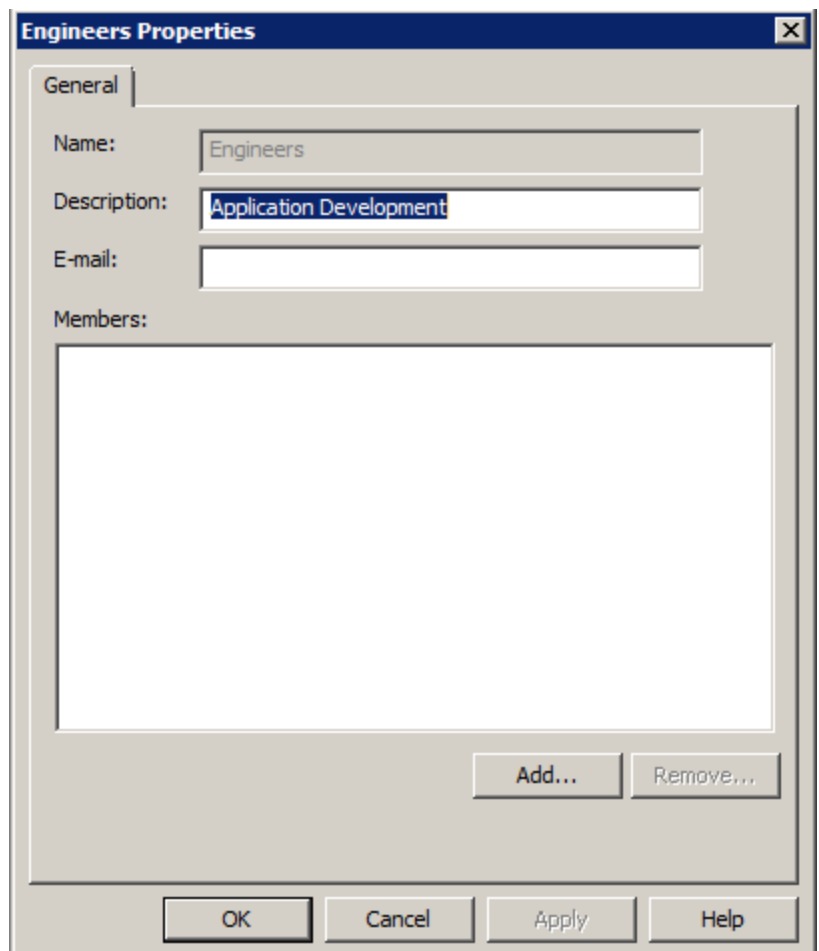


- Type **Engineers** in the name box, and **Application Development** in the description box, and then click **Create**. The Engineers group is added to the User Groups folder.

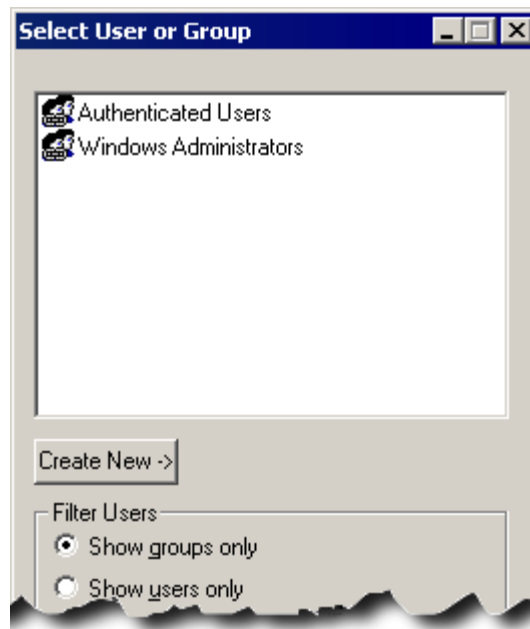


4. Add users to the Engineers group:

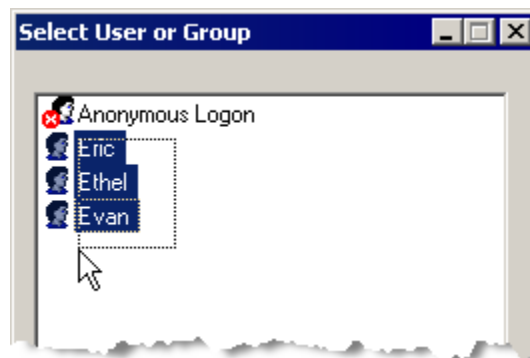
- Right-click the **Engineers** group, and then click **Properties**. The **Engineers Properties** dialog box opens. (For details on using the dialog box, see FactoryTalk Help.)



- Click the **Add** button. The **Select User or Group** dialog box opens.



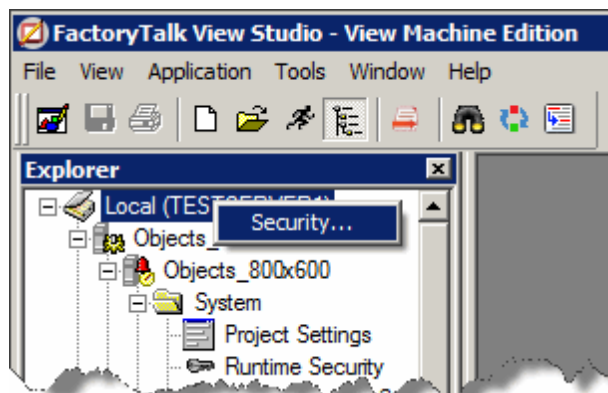
- Click **Show users only** in the Filter Users area near the bottom of the dialog box. All FactoryTalk users, including any Windows-lined users you have added, are displayed.



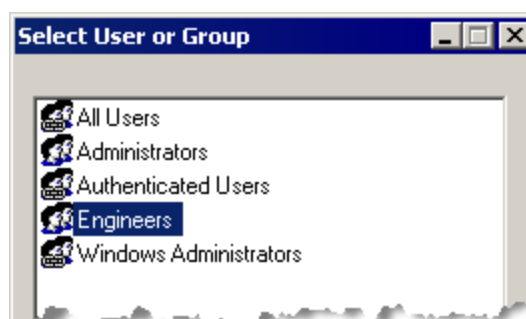
- Select all the users by selecting the first user name and then clicking the left-mouse button plus Shift key on the last user name.
 - Click **OK** to add the users to the Engineers group. All three users display in the **Engineers Properties** dialog box.
 - Click **OK** to close the dialog box and save the changes.
5. Specify actions that users can perform on a resource:

Users defined in a FactoryTalk View application must have, at a minimum, the Common Actions Read and List Children to run a FactoryTalk View project.

- In the Explorer window, right-click the root of the FactoryTalk tree — Local (This Computer) — and select **Security** from the pop-up menu.



- In the 'View permissions by' section of the **Security Settings for Local** dialog box, click the **Add** button. The **Select User or Group** dialog box opens.



- From the **Select User or Group** dialog box, select **Engineers**, and then click **OK**. The Engineers group is added to the list on the **Security Settings for Local** dialog box.
- Expand the list of Common Actions by clicking the plus sign (+) in the left column.
- As shown in the above illustration of the **Security Settings** dialog box, select the check boxes next to **List Children** and **Read**.
This gives the **Engineers** group permission to perform the Common actions *Read* and *List Children* on the FactoryTalk Local Directory. This means that members of the group are able to run the FactoryTalk View ME project.
- Click **OK** to save the settings and close the dialog box.

About multiple System folders in FactoryTalk View

You may notice multiple System folders in the Explorer window. Each HMI project includes its own System folder, and the settings in that folder apply **only** to that specific project. There is also a system folder for the FactoryTalk

Directory. The settings held in the System folder that remains visible and apply to all applications held in the Network or Local Directory.

Which System folder is which? If you are using FactoryTalk View Studio and aren't sure which System folder applies to an HMI project and which applies to all applications in the FactoryTalk Directory, close the area folders in the Explorer tree. The System folder that applies to all applications in the FactoryTalk Directory remains visible in the Explorer tree.

Add FactoryTalk user accounts to FactoryTalk View

After you have created users and groups in FactoryTalk Security, you must add them to the security accounts list in the Runtime Security editor in FactoryTalk View ME. When you add an account, you also assign the security codes that will give those users and user groups access to secured HMI components. (Secured HMI components are those that have been assigned security codes.) These codes (A through P), along with those assigned to HMI project components, determine which components a user has access to at run time.

To restrict access to a graphic display, you assign a security code from **A** through **P** to it, and then assign that code only to the users who are supposed to have access to the component.

For more information about how these features are used in FactoryTalk View, and for examples of assigning FactoryTalk Security permissions to FactoryTalk View users and user groups, see Chapter 11 in the *FactoryTalk View Machine Edition User's Guide, Volume I*.

Example: The following steps use an existing application, Objects_800x600, which is installed with FactoryTalk View.

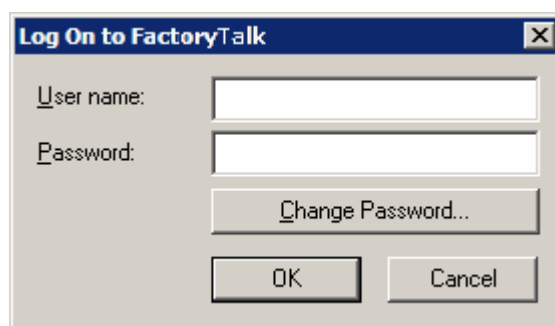
Tip: Be sure to restore the Default back up of the Local FactoryTalk Directory any time you are creating a new application. This ensures that a known Administrator account exists and that you start with a clean directory (no other users have been added).

1. Open FactoryTalk View Studio and add FactoryTalk users or groups to the application:

- From the Windows **Start** menu, select **Rockwell Software > FactoryTalk View > FactoryTalk View Studio**.
- Select **Machine Edition**, and then click **Continue**.
- On the **Existing** tab, select the **Objects_800x600** application, make sure the Language is **English**, and then click **Open**.

The selected application opens in FactoryTalk View Studio, Machine Edition.

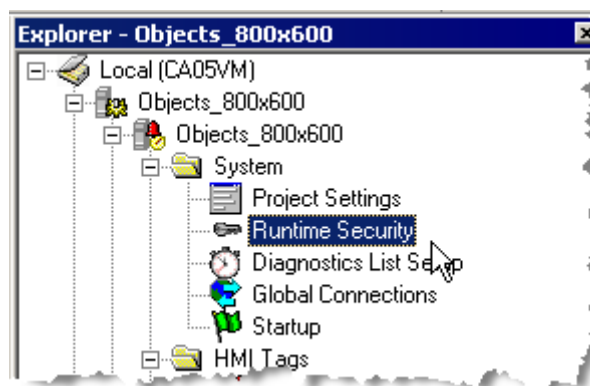
- If prompted to log on to FactoryTalk, enter the name and password of a FactoryTalk user that has administrative rights, and then click **OK**.



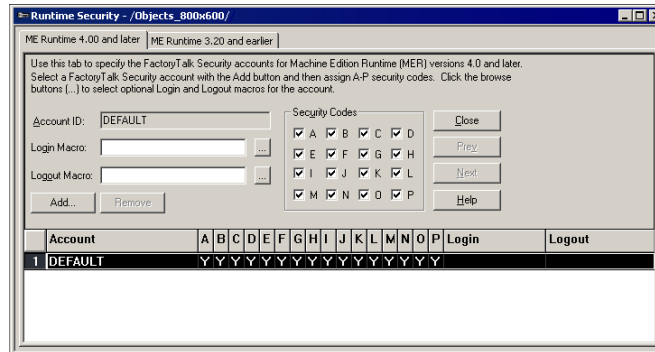
Tip: In FactoryTalk Security CPR 9 or later, single sign-on is enabled by default, so users are not prompted to log on to FactoryTalk. If you are upgrading from CPR 7, or if you changed the default FactoryTalk security configuration, you may be prompted to log on.

2. Open the Runtime Security editor:

- In the FactoryTalk View Studio Explorer window, select **Runtime Security** from the **System** folder.



The Runtime Security editor opens.



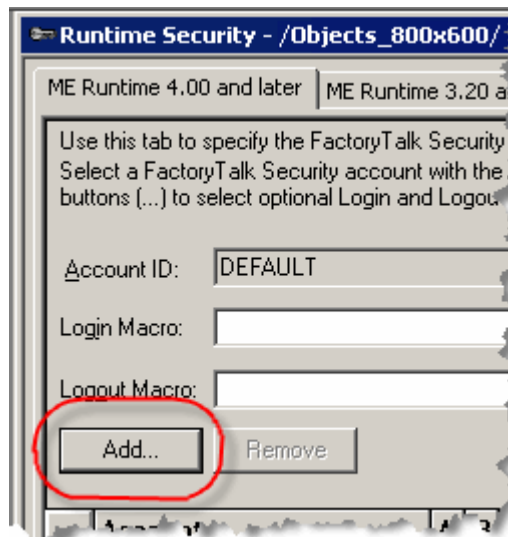
The first account in the editor is the **DEFAULT** user account. The DEFAULT account is used when no one is logged in. The DEFAULT user initially has access to all security codes (A-P). Unless you want everyone to have access to all parts of the application at run time without logging in, turn off the DEFAULT user's access to the all the security codes you plan to use. See Help or Chapter 11 of the *FactoryTalk View Machine Edition User's Guide, Volume 1*.

You cannot delete the DEFAULT user account.

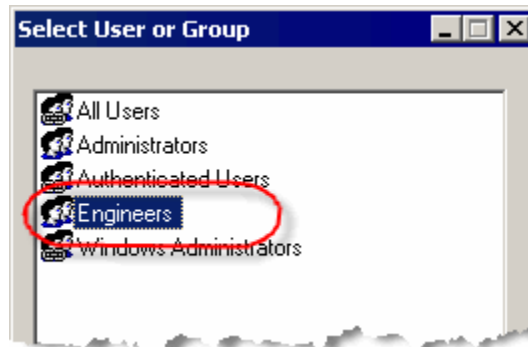
Important: Assign the security code for the startup display to the DEFAULT user, or else the startup display won't open. If the startup display uses the * security code, you can assign any code from A to P to open the display.

3. Assign rights to the Engineering role:

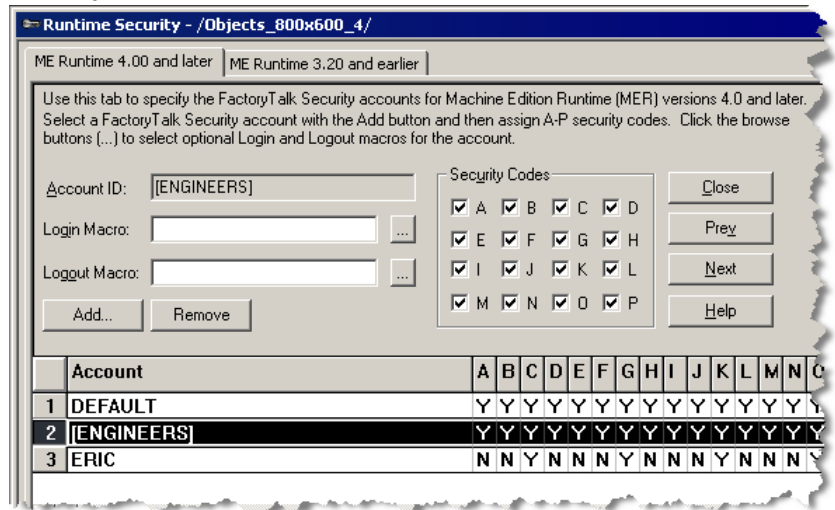
- On the **ME Runtime 4.00 and later** tab of the Runtime Security editor, click the Add button.
- In the Runtime Security editor, click the **Add** button to open the **Select User or Group** dialog box.



- In the **Select User and Computer** dialog box, click the name of a user or group to be added to the Runtime Security user accounts list, and then click **OK**. For this example, select **Engineers**.

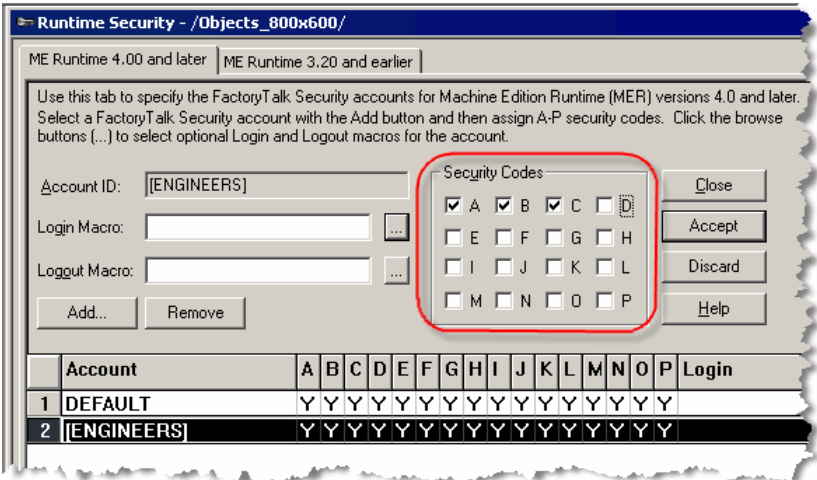


The Engineers group is added to the list of accounts in the Runtime Security editor.



Tip: If a FactoryTalk user account has been deleted from the FactoryTalk Directory's System folder, the user's unique identifier remains and will display as an alphanumeric string in the Runtime Security editor. See [Deleting user accounts](#) on [page 76](#) for details.

- In the Runtime Security editor, select the **Engineers** group and clear all of the boxes in the Security Codes area, except for **A**, **B**, and **C**, as shown below.

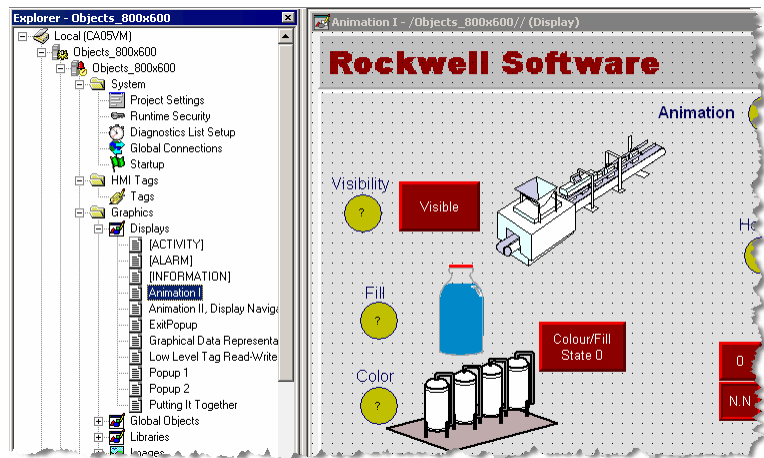


Any user in the Engineers group now has run-time access only to graphic displays that have an A, B, or C security code assigned.

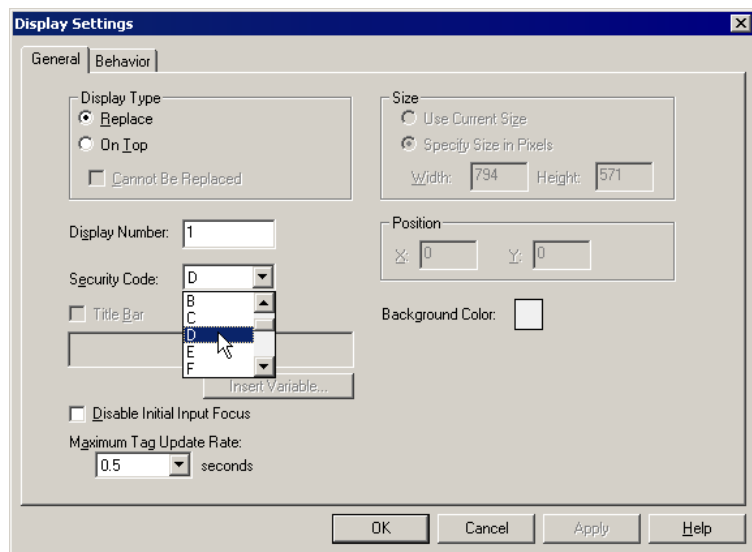
- Click **Accept**.
- In the **Runtime Security** editor, you can also specify login and logout macros for the user or group you have just added, if desired. Refer to FactoryTalk View Machine Edition Help or Chapter 11 of the FactoryTalk View Machine Edition User's Guide.
- Click the **Close** button to close the **Runtime Security** dialog box. Click **Yes** to save changes.

4. Set security on a display:

- In the Explorer window, expand **Graphics > Displays** and double-click **Animation 1** to open it.



- From the **Edit** menu, select **Display Settings**. The **Display Settings** dialog box opens.

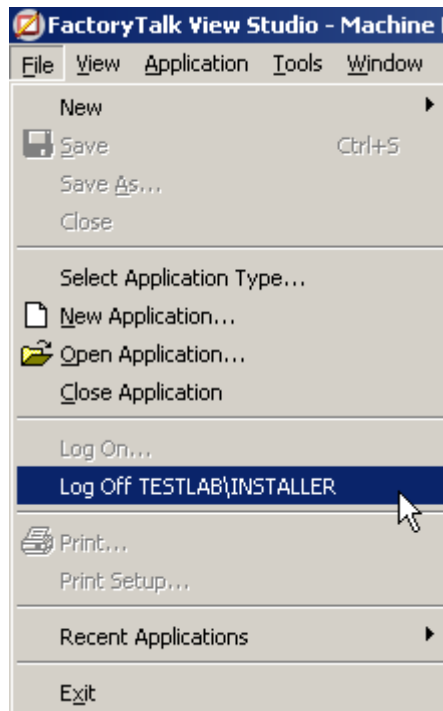


From the **Security Code** drop-down list on the **General** tab, select **D** (or a code that you **have not** assigned to the Engineers group), and then click **OK** to save the change and close the dialog box. Save the application by selecting **Save** from the **File** menu.

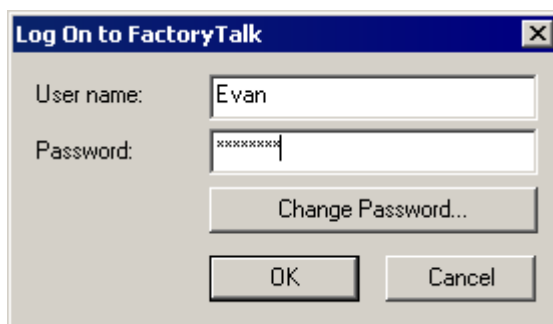
- Test the application:



- On the **Application** menu, click **Test Application**, or click the **Test Application** button.
 - If your application uses multiple languages, specify the languages to include and the initial runtime language, and then click **Finish**.
 - When the application opens, click the **Next** button twice to navigate to the Animation display.
 - Stop the application by clicking the **Exit** button on the application display (or by pressing the **F4** key on your keyboard).
6. Now log off of FactoryTalk, log back on as **Evan**, and then test run the **Objects_800x600** application:
- From FactoryTalk View Studio, select **Log Off** from the **File** menu.



- Click **Yes** to close the application.
- To log on as **Evan** (a member of the Engineers group), select **Log On** from the **File** menu.
- Enter **Evan** as the User name, type **password** in the Password box, and then click **OK**.

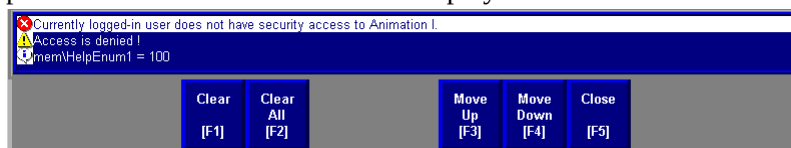


- In the New/Open Machine Edition Application dialog box, select the **Objects_800x600** application, select **English** as the default language, and then click **OK**.



- On the **Application** menu, click **Test Application**, or click the **Test Application** button.
- When the runtime application opens, click the **Next** button twice to navigate to the Animation display.

Note that as a member of the Engineers group you do not have permission to view the Animation display.



- Stop the application by clicking the **Exit** button on the application display (or by pressing the **F4** key on your keyboard).

Managing FactoryTalk Security for multiple applications

There are two main usage categories for FactoryTalk Security in a FactoryTalk View Studio application; Runtime and Development. This section focuses on how to maintain the security settings for both categories.

Runtime security relates to who can be authenticated to view a running application and what actions/displays they are authorized for. An example action would be starting a FactoryTalk View application into runtime or which displays an operator has access to.

Development security relates to who can be authenticated to edit an application and what actions they are authorized to do. An example action would be archiving or restoring a FactoryTalk View application.

When multiple applications are being configured on the same computer, great care must be taken when working with FactoryTalk Security. The runtime security user list and settings are contained within each application itself. However, the runtime user list actually references the users and groups within the FactoryTalk directory. There can only be one active FactoryTalk directory on a computer (development or runtime).

Back up the development application

A FactoryTalk View application does not actually contain users or groups. It simply contains a list of references to the FactoryTalk directory users/groups. The FactoryTalk View application also holds the runtime security rights for the referenced users/groups.

When an application backup is performed the FactoryTalk View application files, the user accounts runtime access rights and the FactoryTalk directory are compiled into the APA backup file.

On the development computer, back up the application. Follow the steps below:

- a. From the Windows **Start** menu, select **All Programs > Rockwell Software > FactoryTalk View > Tools > Application Manager**.
- b. From the Application Manager, select **Machine Edition** and then click **Next**.
- c. Select **Backup application** and then click **Next**.
- d. Select the application to back up and then click **Next**.
- e. Enter the required information for the application and then click **Finish**.

Each application backup file (.apa) contains a copy of the FactoryTalk directory that was active at the time of backup. It is very common for different applications to have a different set of users and groups based on the FactoryTalk directory the application was created with. This results in a different FactoryTalk directory for each .apa backup file.

Back up runtime application and FactoryTalk Local Directory

To do this, follow the steps below:

1. On the development computer, back up the runtime application. The steps are same with steps to back up the development application. For details see page 152.



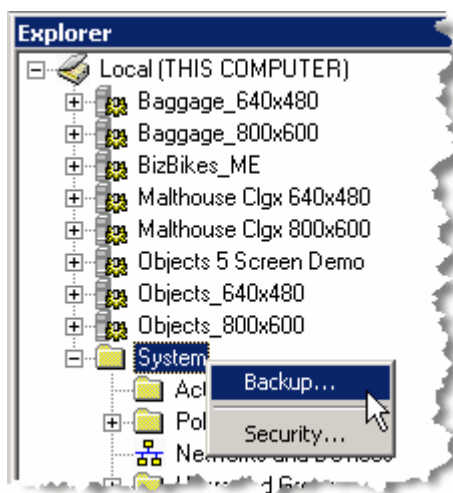
This step is critical, especially if you are developing applications for multiple clients. Backing up any existing applications allows you to not only restore your client's FactoryTalk View applications to their original state, but it also allows you to restore that client's FactoryTalk Local directory should that get overwritten.

2. (optional) On the development computer, back up the FactoryTalk Local Directory . Follow the steps below:

Important: While this step is optional when you back up an application from the Application Manager, it is very good idea. There can be one FactoryTalk Local Directory to many FactoryTalk View Applications, so you should back up the FactoryTalk Local Directory if you have multiple applications referencing the Directory.

If there is one FactoryTalk Directory to one FactoryTalk View ME application, then the back up created with the Application Manager (.apa) will contain the FactoryTalk Local Directory.

- a. Open FactoryTalk View Studio or FactoryTalk Administration Console.
- b. In the Explorer window, right-click the FactoryTalk Directory System folder and then select Backup from the context menu.



- c. On the Backup dialog box, enter the required information for the backup file and then click OK.

Important: It is highly recommended that you use a new file name each time to create versions of your FactoryTalk View ME application backups. This allows you to revert to older versions if needed

- d. Use Windows Explorer to save a copy of the .bak file to another location off the local computer (to a CD, network PC, or USB memory stick, for example).

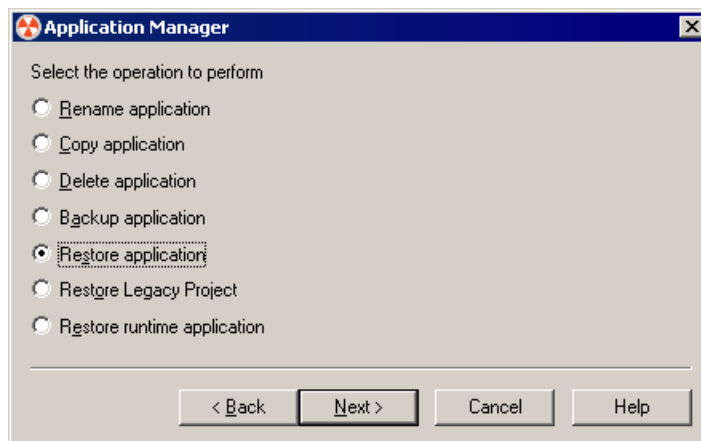
Restore the application to the runtime computer

Before restoring the application, copy the backed up application from the development computer to the runtime computer.

Note: Always back up your FactoryTalk View SE (local) and Machine Edition applications and your Local FactoryTalk Directory before you restore any applications and/or the FactoryTalk Directory.

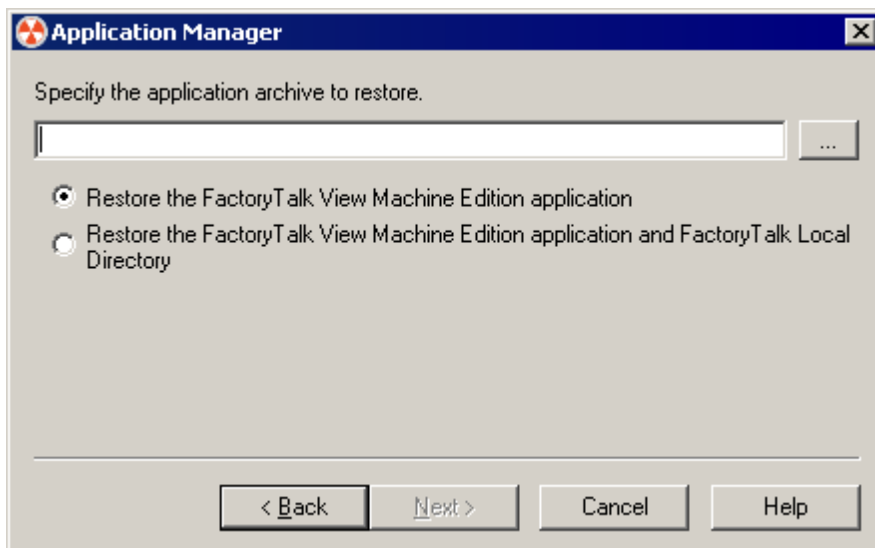
To restore the application:

1. From the Windows **Start** menu, select **All Programs > Rockwell Software > FactoryTalk View > Tools > Application Manager**.
2. From the Application Manager, select **Machine Edition** and then click **Next**.
3. Select **Restore application** and click **Next**.



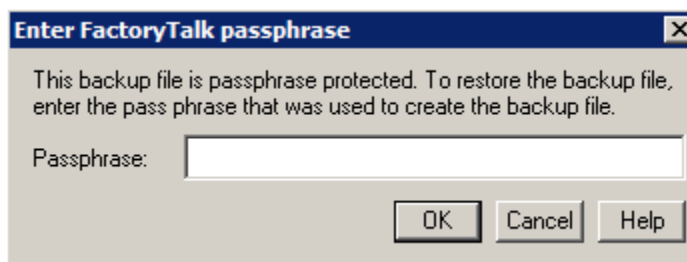
Important: When you perform an application restore, the Application Manager provides you with the option to restore the FactoryTalk directory from the .apa file.
If you choose to restore the FactoryTalk directory, the currently loaded directory on the local computer will be overwritten.

4. Select the application to restore, select **Restore the FactoryTalk View Machine Edition application** and then click **Next**.



You can also choose to restore both the application and the FactoryTalk Local Directory. Be sure you have first backed up all FactoryTalk View SE (local) and Machine Edition applications on this computer before proceeding. The current FactoryTalk Local Directory, including users, groups, and policies, will be replaced with the Local FactoryTalk Directory contained in the .apa file selected. This affects all other FactoryTalk-enabled programs and applications running on this computer.

5. If the backup file was encrypted, enter the passphrase that was used during the backup operation and click **OK**.



6. Enter a new name for the application being restored and then click **Finish**.

Working with the 3.20 user account tab

In some cases, the customer assign rights to user roles (not to be confused with role-based security). In user roles, individual user accounts are created to represent the roles. All users in a particular role log on with one of the user role accounts.

Important: This only works for user-based security. Some customers assign rights to individual user accounts like Eric, Evan and Ethel, for example

Creating and storing these types of user accounts in the 3.20 user account tab allows the migration to 4.x accounts.

Tip: Here's a cool tip: Add your users and groups to the **3.20 and earlier** tab, assign security codes and optional login or logout macros to those users, and then import them into the **4.00 and later** tab. This preserves the users you have assigned to the application, which means they will be available to import again should the application or FactoryTalk Directory get restored from a back up file that does not contain those users.

Example: In the following steps, user accounts (not user groups) named Eng, Main, and Opr will be created. All engineers will log on to the same user role, Eng. Following the engineering example used in the previous section, users Eric, Evan and Ethel would all log on the same user account, Eng, with the same password.

- The Runtime Security editor opens. Select the **ME Runtime 3.20 and earlier** tab.
- In the Runtime Security editor, double-click any row in the table to add a new user or group.

Runtime Security - /Objects_800x600_4/

ME Runtime 4.00 and later ME Runtime 3.20 and earlier

Use this tab to specify the accounts for Machine Edition Runtime (MER) versions 3.20 and earlier. The accounts defined in this tab are specific to this application.

Account ID:

Login Macro: ...

Logout Macro: ...

Password:

Security Codes

☒ A ☒ B ☒ C ☒ D

☒ E ☒ F ☒ G ☒ H

☒ I ☒ J ☒ K ☒ L

☒ M ☒ N ☒ O ☒ P

Close

Prev

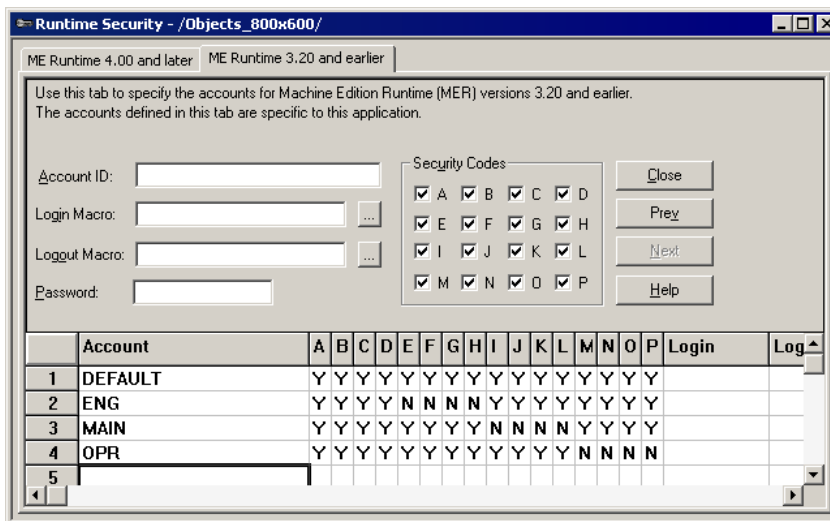
Next

Help

	Account	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Login	Logout
1	DEFAULT	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
2																			
3																			
4																			

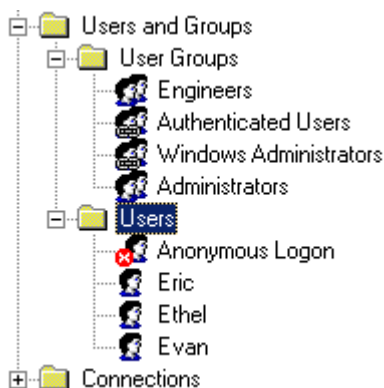
- In the Account column, type **Eng**.

- Type **password** in the Password box, and then click the **Accept** button. The user role **Eng** is added to the application. Uncheck the E, F, G, and H security codes.
- Add the user roles **MAIN** and **OPR** to the editor and assign security codes as shown below. Remember, these are user accounts not groups.



In the **Runtime Security** editor, you can also specify login and logout macros for the user or group you have just added, if desired. Refer to Help or Chapter 11 of the *FactoryTalk View Machine Edition User's Guide, Volume 1*.

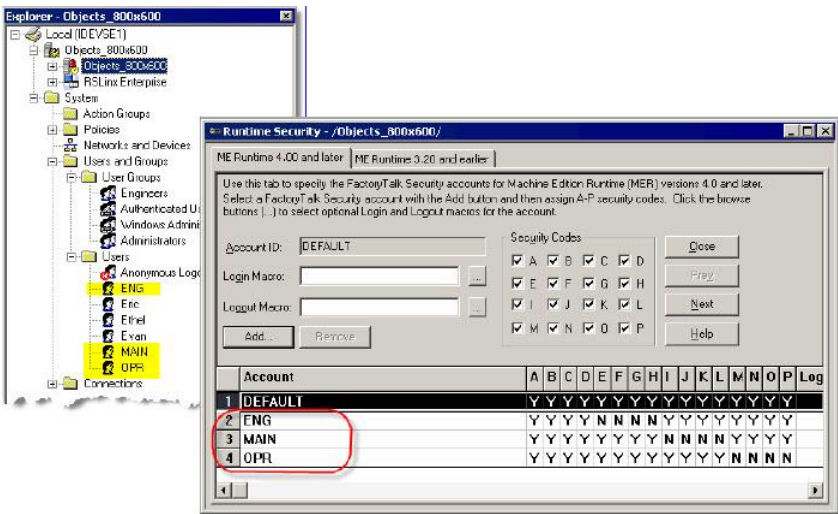
- Click the **Close** button to close the **Runtime Security** dialog box. Click **Yes** to save changes.
1. Migrate the 3.20 user accounts to the **4.00 and later** tab:
 - Open the Runtime Security editor and select the **ME Runtime 4.00 and later** tab. Note the user accounts you just created (ENG, MAIN, and OPR) do not exist on this tab.
 - Also note that the ENG, MAIN, and OPR user accounts do not exist in the FactoryTalk Directory:



- From the **Setup** menu, select **Migrate ME Runtime 3.20 and earlier accounts**.



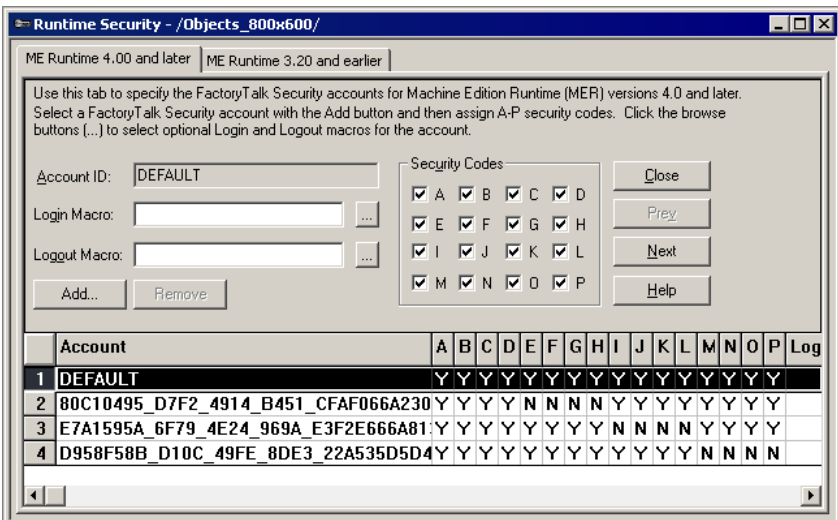
The user accounts are created in the FactoryTalk Directory and added to the ME Runtime 4.0 tab.



- Close the Runtime Security editor; click **Yes** to save the settings.

If the customer did not restore the FactoryTalk Directory with the application or the user accounts were deleted, the user accounts stored on the 3.20 tab could be migrated back into the application.

The Runtime Security editor would look like this if the original accounts were deleted:



Tip: If a FactoryTalk user account has been deleted from the FactoryTalk Directory's System folder, the user's unique identifier remains and will display as an alphanumeric string in the Runtime Security editor. See [Deleting user accounts](#) on [page 76](#) for details.

1. Migrate the accounts again:

- From the **Setup** menu, select **Migrate ME Runtime 3.20 and earlier accounts**.

The new user accounts matching the original accounts have been created in FactoryTalk and the Runtime Security editor:

Account	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Log
1 DEFAULT	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
2 80C10495_D7F2_4914_B451_CFAF066A230	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
3 D958F58B_D10C_49FE_8DE3_22A535D5D4	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
4 E7A1595A_6F79_4E24_969A_E3F2E666A81	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y	Y
5 ENG	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
6 MAIN	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y	Y	Y
7 OPR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N

2. Delete the orphaned user GUIDs:

- Select the GUID in the Runtime Security editor, and then click the **Remove** button.

Account	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Log
1 DEFAULT	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
2 ENG	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
3 MAIN	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y	Y	Y
4 OPR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N

3. Exit the Runtime Security editor and save the changes.

Where to go from here

Now that you've set up security for FactoryTalk View, do one of the following:

- Log in as an administrative user and continue assigning permissions for graphic displays, if desired.
- Go to [RSLink and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLink software.
- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure projects.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk Batch and FactoryTalk Security](#) on [page 201](#) to learn how to use FactoryTalk Security with FactoryTalk Batch components

- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.

FactoryTalk Batch and FactoryTalk Security

This section explains administering security for the FactoryTalk® Client components using FactoryTalk Security.

Tip: For information on the administration of your FactoryTalk Security system as a whole, see **FactoryTalk Help** located in the FactoryTalk Administration Console. For detailed information on using FactoryTalk Security with the FactoryTalk Batch Clients, see the *FactoryTalk Batch Administrator's Guide*, available from the Windows **Start** menu: **Start > Rockwell Software > FactoryTalk Batch Suite > Online Books > Batch > batch_administrator.pdf**.

FactoryTalk Batch product policies are created in the Local Directory and the Network Directory when the FactoryTalk Services Platform installs. The FactoryTalk Batch product policies are used to restrict access to the FactoryTalk Batch client components and the features within them. For a complete list of FactoryTalk Batch secured resources and their default product policy settings, see "FactoryTalk Batch Default Policy Settings" in Chapter 3 of the *FactoryTalk Batch Administrator's Guide*.

Before you begin

- Identify the computers that will be configured as the FactoryTalk Batch Server and FactoryTalk Batch Client.
- FactoryTalk Batch, v. 9.0 (CPR 9) or later
- Become familiar with the terms and concepts of FactoryTalk Security. See [Understanding automation security](#) on [page 17](#) and [About the FactoryTalk system](#) on [page 21](#) for more information.
- Install and configure the software listed in "What you need", below.

What you need

On the computer acting as the FactoryTalk Batch Server (**Computer1** in our sample scenario):

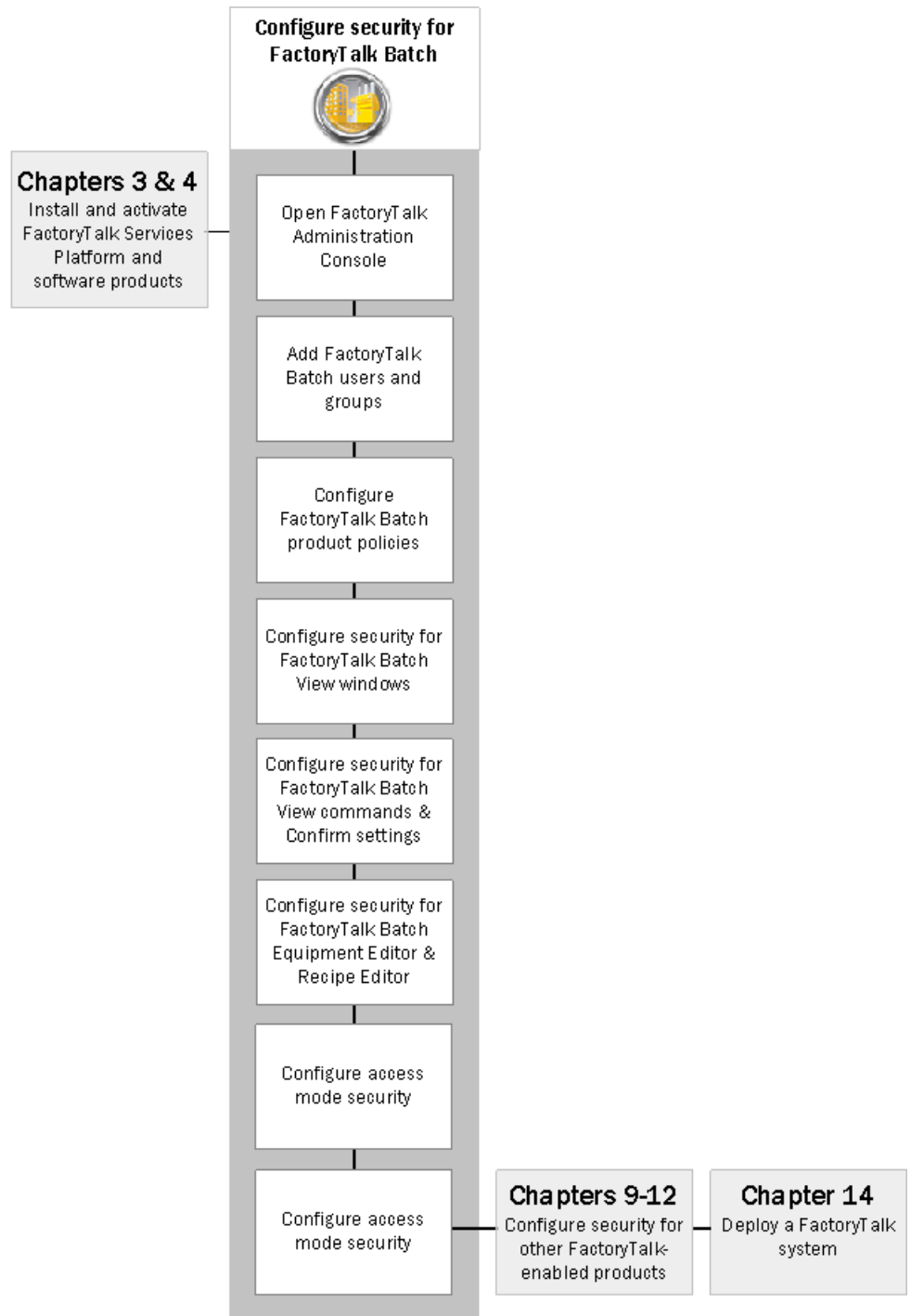
- FactoryTalk Services Platform v. 2.10 (CPR 9) or later. Using the newest available version is recommended.
- FactoryTalk Activation
- FactoryTalk Batch Server components

On the computer acting as the FactoryTalk Batch client (**Computer2** in our sample scenario):

- FactoryTalk Services Platform v. 2.10 (CPR 9) or later

- FactoryTalk Activation
- FactoryTalk Batch client components, including FactoryTalk Batch View, Equipment Editor and Recipe Editor

Follow these steps



Some important information on installing FactoryTalk Batch

You must create a Windows user account for the FactoryTalk Batch Server prior to installing the FactoryTalk Batch applications. When you install FactoryTalk Batch and RSBizWare eProcedure applications you are prompted to enter this user account to allow the installation program to configure your FactoryTalk Batch system.

When creating the Server user account, the following configuration

requirements must be met.

- **The password should be configured to never expire** – If the password ever expires, the Batch Server service eventually fails to log on.
- **The Server user account should never be disabled or deleted** – If this account is ever disabled/deleted, the Batch Server service eventually fails to log on.
- **The domain user account should have a unique name** – If the Server user account is a domain account, remove any local user accounts with the same name.
- **The Server user account/user group must exist on all workgroup computers** – If you are using a local account and expect that account to have access to resources on other computers in a workgroup environment, you must create accounts with the same name and password on each computer in the workgroup.

Refer to the FactoryTalk Batch Installation Guide and the FactoryTalk Batch Administrator's Guide for detailed information on installing FactoryTalk Batch. These books are available from selecting **Start > All Programs > Rockwell Software > FactoryTalk Batch Suite > Online Books > Batch**

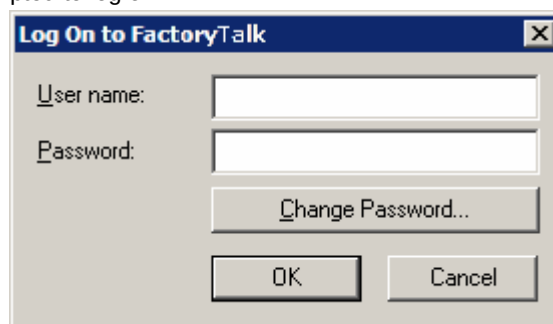
Create FactoryTalk Batch users and groups

Once you have installed FactoryTalk Services Platform and FactoryTalk Batch, you can tighten security by adding users and user groups to FactoryTalk Security. For detailed information about creating users and user groups in FactoryTalk Security, see the FactoryTalk Security Help.

On the Batch Server computer (Computer1 in this example):

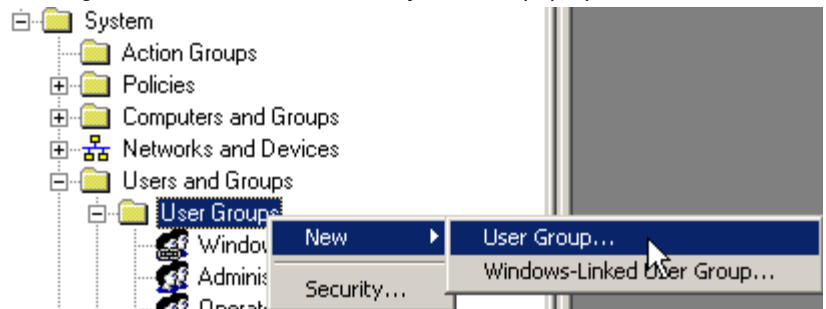
1. Create a *user group* account in FactoryTalk Security:
 - To open FactoryTalk Administration Console, click **Start > Rockwell Software > FactoryTalk Administration Console**.
 - If prompted to log on to FactoryTalk, enter a valid FactoryTalk administrator user name and password, and then click **OK**.

Tip: In FactoryTalk Security CPR 9, single sign-on is enabled by default, so users are not prompted to log on to FactoryTalk. If you are upgrading from CPR 7, or if you changed the default FactoryTalk security configuration, you will be prompted to log on.

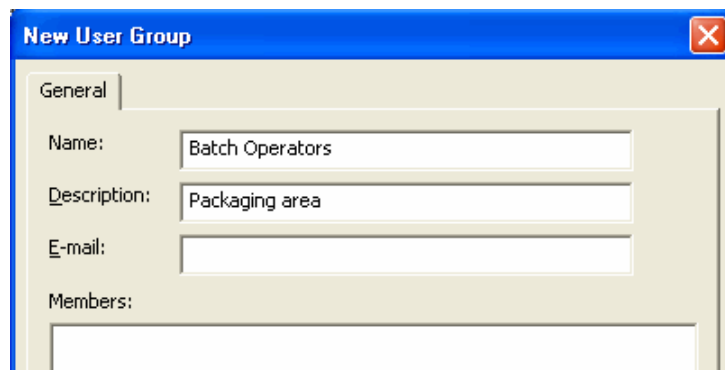


- In the Explorer window, expand the **Users and Groups** subfolder in the **System** folder.
- Right-click the **User Groups** folder, point to **New** and then select **User Group** from the pop-up menu.

Tip: If you have an existing Windows user group, you can add a security account for it by selecting **Windows-linked User Group** from the pop-up menu.



- Type a **Name** and **Descriptor** (we used **Batch Operators** for this example).

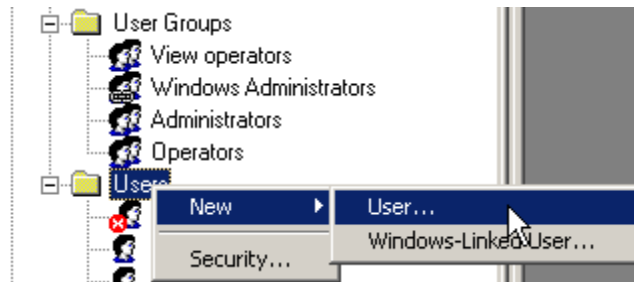


- Click **Create** to create the security account for the user group and close the dialog box. When you double-click the **User Groups** folder to open it, you will see the user group you just added.

2. Create a new *user* account in FactoryTalk Security:

- In the Explorer window, expand the **Users and Groups** subfolder in the **System** folder.
- Right-click the **Users** folder, point to **New**, and then select **User** from the pop-up menu.

Tip: You can add existing Windows users by selecting **Windows-linked User**.



- In the **General** tab of the **New User** dialog box, specify the user's login name and password, and other information as necessary.

For details about the options in the dialog box, click the **Help** button.



For this example, enter the following:

User name: **SWhite**

Full name: **Sara White**

Description: **Operator**

Password: **password**

For this example, clear the **User must change password at next logon** check box, and then select the **Password never expires** check box.

3. Associate a group with the user account.

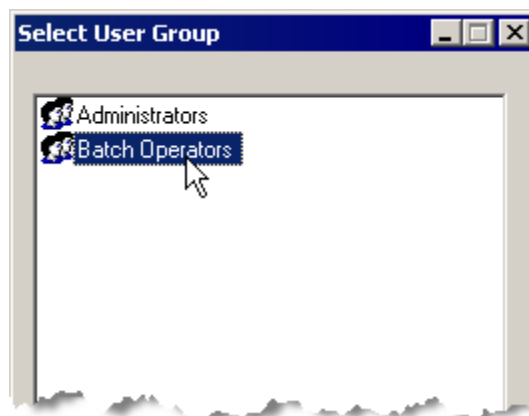
You can add users (members) to groups in two ways. You can select a group and add members to it, or you can associate one or more groups

with a user when you create a new user. The following steps use the second method.

- Click the **Group Membership** tab of the **New User** dialog box. (This dialog box should still be open. If not, right-click the user you just created and select **Properties** from the pop-up menu.)



- Click the **Add** button on the **Group Membership** tab to open the **Select User Group** dialog box.



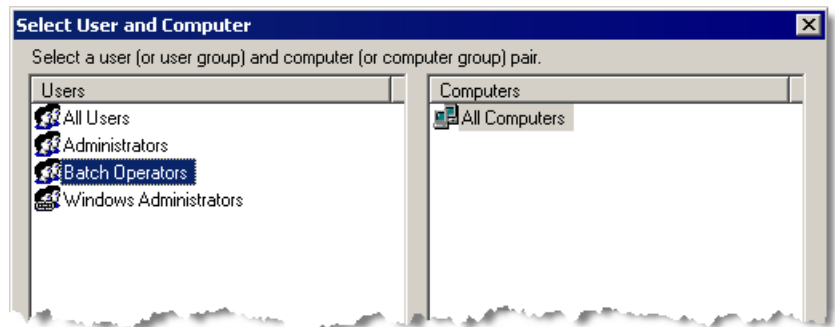
- Select the user group you created in step 2 (our example used **Batch Operators**), and then click **OK**.
- Click **Create**. The new user appears in the **Users** folder.



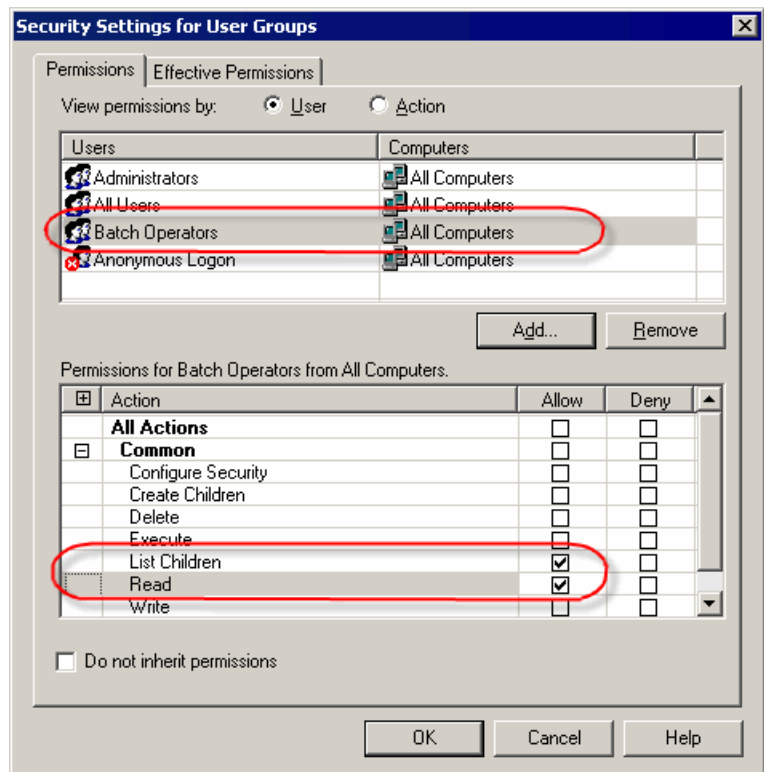
4. Specify actions that users can perform at the application level:

To secure access to an application, specify which users or groups of users have permission to perform actions.

- In the Explorer window, open the application that you want to secure.
- Right-click the application folder, and then select **Security** from the pop-up menu.
- In the 'View permissions by' section of the **Security Settings for User Groups** dialog box, click the **Add** button.



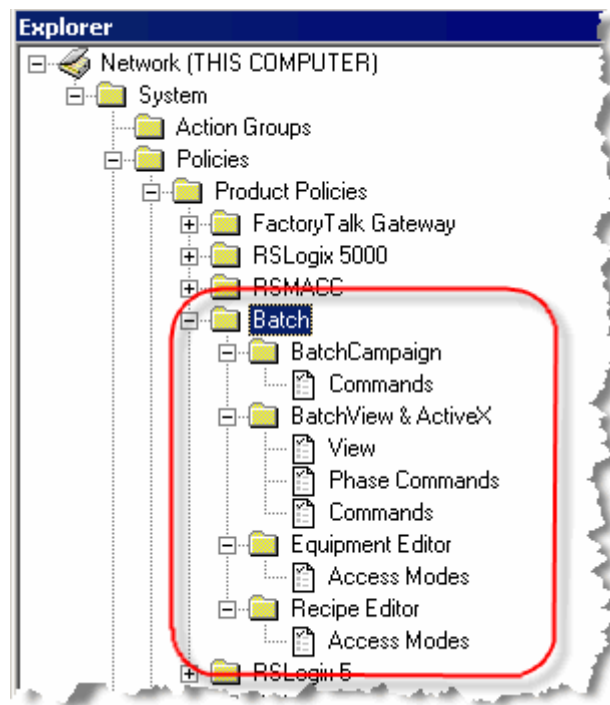
- For this example, select **Batch Operators**, and then click **OK**. The Batch Operators group is added to the list.
- With the Batch Operators group selected, expand the list of Common actions by clicking the plus sign (+) in the left column.



- As shown in the above illustration of the **Security Settings** dialog box, select the check boxes next to **List Children** and **Read**.
- Click **OK** to save the settings and close the dialog box.

Configure FactoryTalk Batch Product Policies

The FactoryTalk Batch clients (BatchCampaign, Batch View, Equipment Editor, Recipe Editor, and the Batch ActiveX controls) have product policies that can be secured with FactoryTalk Security.



For example, you can configure FactoryTalk Security to specify which FactoryTalk Batch View toolbar buttons and windows are available to specific users or groups of users. Removing a user group from a security policy disables the corresponding View toolbar button for all users who are members of that user group. When a button is disabled, it no longer appears on the FactoryTalk Batch View toolbar.

Additionally, you can restrict access to resources based on where a user is physically located, such as a computer used to perform actions. (*For more information see FactoryTalk Help.*)

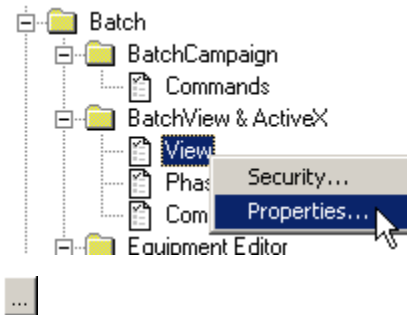
Configuring security for the FactoryTalk Batch View windows

To tighten security for a FactoryTalk Batch View window, configure the corresponding product policy in the appropriate FactoryTalk Directory.

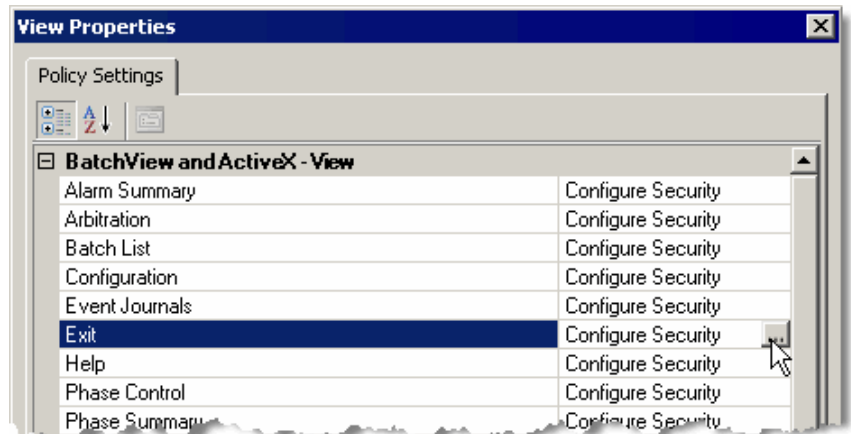
On the Batch Server computer (Computer1 in this example):

1. Open the FactoryTalk Administration Console and log on to the appropriate FactoryTalk Directory. For this example, select the **Network Directory**.
2. Configure security for the FactoryTalk Batch View windows:

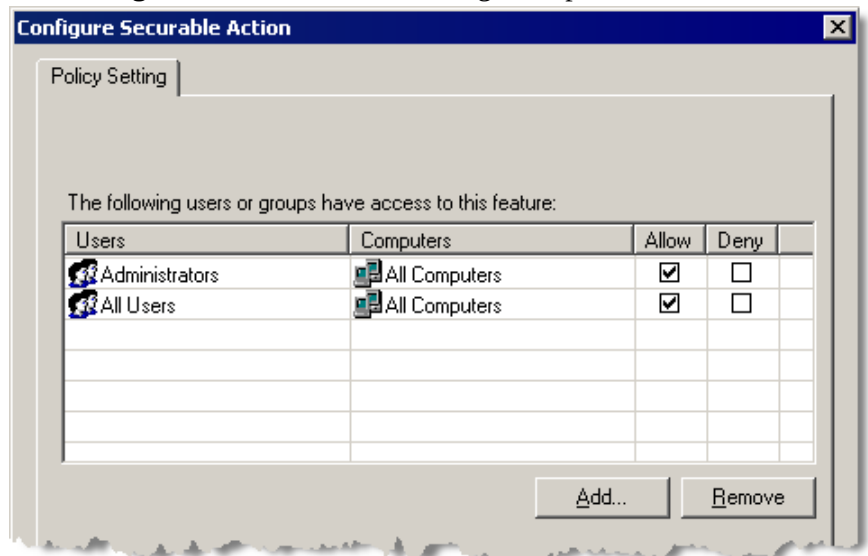
- Expand **System > Policies > Product Policies > Batch > BatchView & ActiveX** and then right-click on **View** and select **Properties**.



- From the **View Properties** dialog box, select the policy setting you want to configure and click the corresponding browse button. For this example, click the browse button for the Exit policy.



The **Configure Securable Action** dialog box opens.



- Click the **Add** button. The **Select User or Group** dialog box opens. Select the user or group you want to add and click **OK**. For this example, select the **Batch Operators** group.
- To allow the group access to the feature, select the **Allow** check box.

Important: Product policies do not inherit security settings. When specifying permissions for product policies, clearing both the **Allow** and **Deny** check boxes denies access to the product feature. *(For more information on permissions see FactoryTalk Help.)*

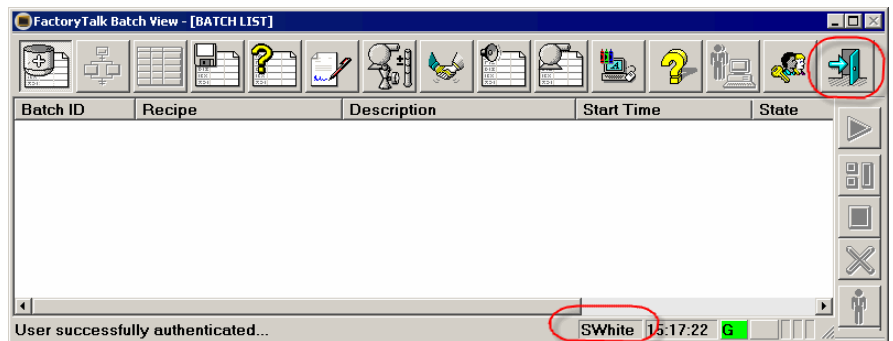
3. Tighten security for this command:

- Select the **All Users** group and click **Remove**.
- Click **OK** twice to return to the FactoryTalk Administration Console.

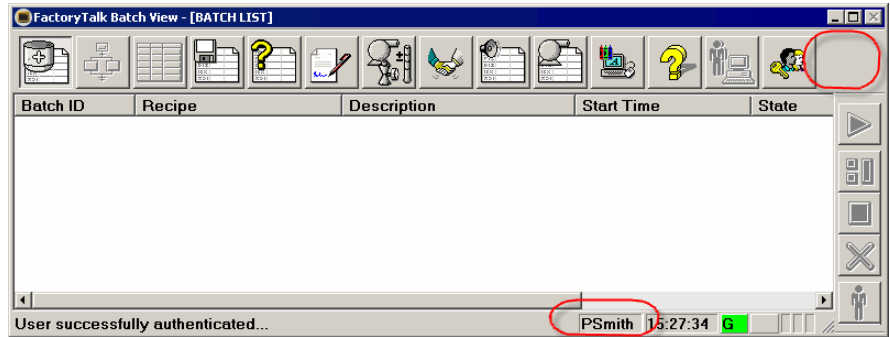
Important: Restart all open FactoryTalk Batch components to update changes made in the FactoryTalk Directory.

4. Test the policy setting:

- Open FactoryTalk Batch View and log in as log in as **SWhite** (the password is **password**). Note that the status bar shows SWhite as the currently logged in user and the **Exit** button is on the toolbar:



- Now click the **Log In** button (shown at left) and log in as **PSmith** (the password is **password**). Note that the status bar shows PSmith as the currently logged in user, and the **Exit** button is no longer displayed on the toolbar:



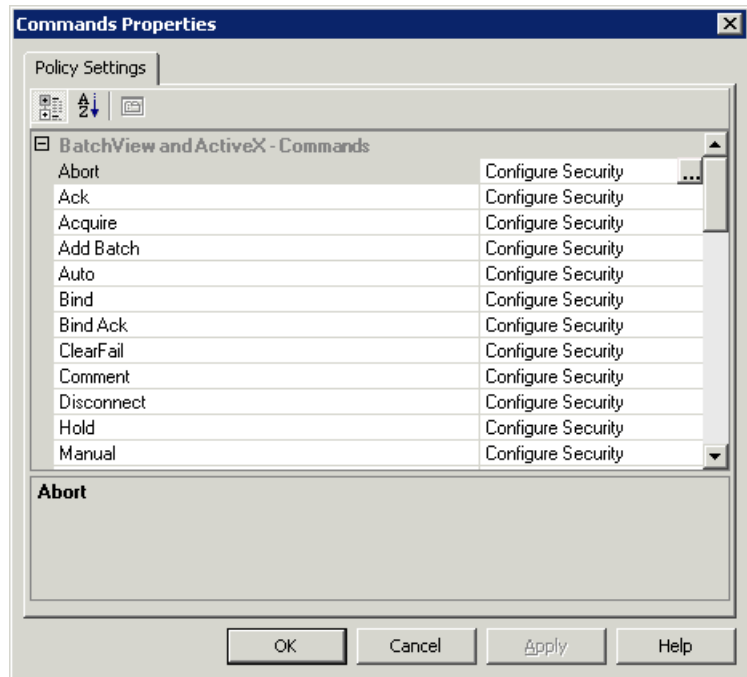
- Log in as a FactoryTalk administrator, or as a user who has access to the Exit policy, and you will be able to close the program.

Configuring Security for FactoryTalk Batch Commands

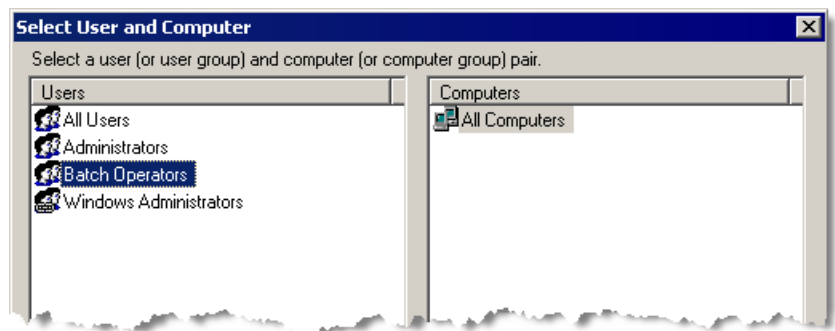
In addition to securing access to various windows and buttons in the FactoryTalk Batch View, you can opt to allow only specified users to issue commands against a batch or a phase. Add the appropriate users and/or user groups to the **Command** or **Phase Command** policy setting you want to secure.

1. To add a user and/or user group to a **Command** policy setting:

- Open the FactoryTalk Administration Console and log on to the appropriate FactoryTalk Directory. This example uses the **Network Directory**.
- Expand **System > Policies > Product Policies > Batch > BatchView & ActiveX**.
- Right-click on **Commands** (or Phase Commands) and select **Properties** from the pop-up menu. The **Commands Properties** dialog box opens.



- Select the policy setting you want to configure and click the corresponding browse button. For this example, select **Add Batch**. The **Configure Securable Action** dialog box opens.
- To add a user or group select **Add**. The **Select User and Computer** dialog box opens.



- Select the user or group you want to add and click **OK**. For this example, select **Batch Operators**.

2. Tighten security for this command:

- Select the **All Users** group and click **Remove**.
- Click **OK** twice to return to the FactoryTalk Administration Console.

Tip: Restart all open FactoryTalk Batch components to update security changes made in the FactoryTalk Directory.

3. (*Optional*) Log in to FactoryTalk Batch View as **SWhite** and attempt to add a batch to the batch list. Then log in as **LWilliams**, who does not have permission to add a batch, and try adding a batch to the batch list. You will be prompted that the user does not have sufficient rights to perform the command.

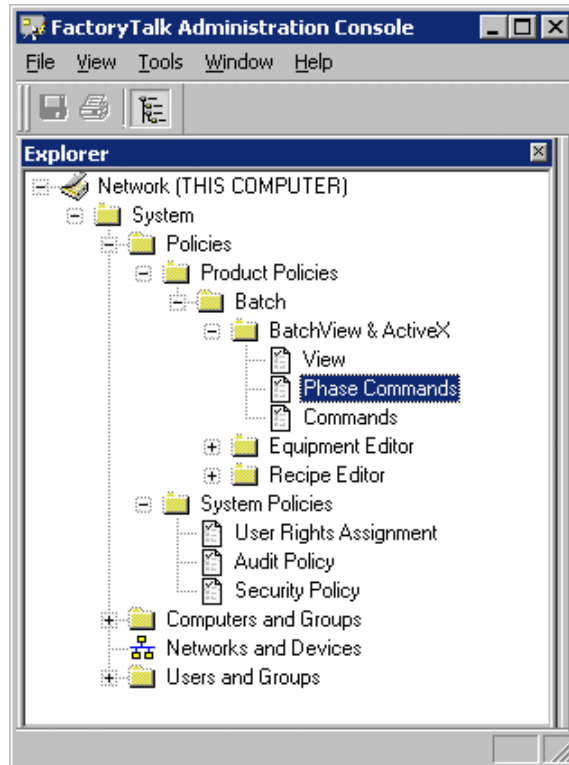
Enabling FactoryTalk Batch View Confirm Settings

If you assign specific users and/or groups to a batch command or phase command and enable the corresponding Confirm policy setting, then only the specified users are allowed to issue the command and they will be required to enter a user name and password to confirm the command being initiated.

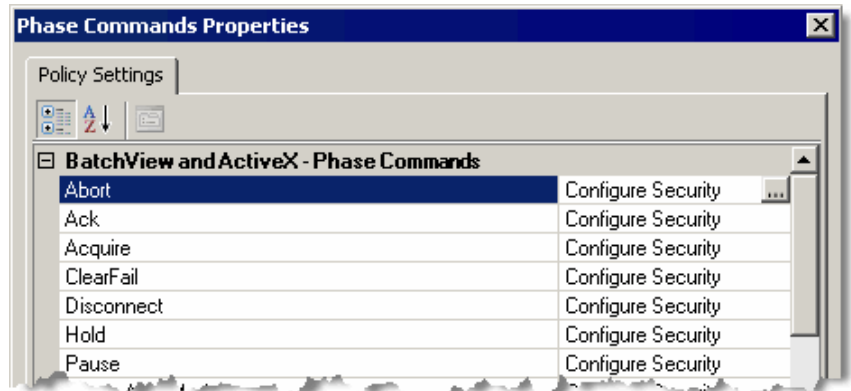
1. Configure **Phase Command** policy settings:

Tip: To configure Command Confirm policy settings substitute Commands for Phase Commands in the following steps.

- Open the FactoryTalk Administration Console and log on to the appropriate FactoryTalk Directory. This example uses the **Network Directory**.
- Expand **System > Policies > Product Policies > Batch > BatchView & ActiveX**.

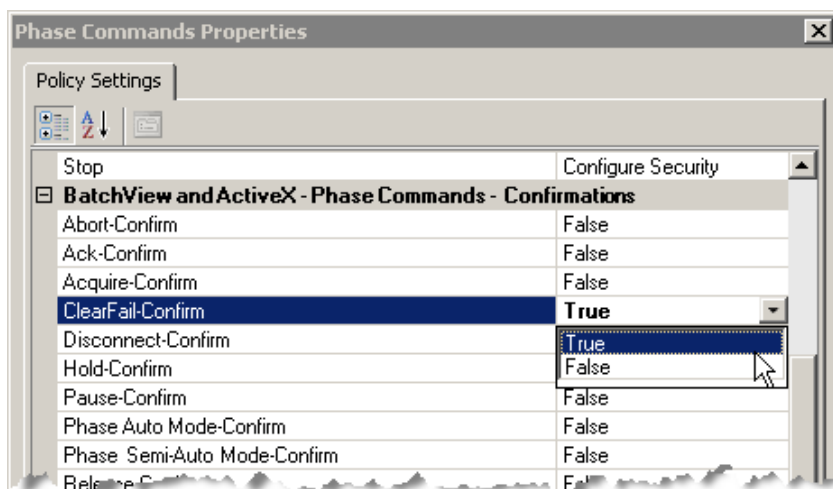


- Right-click **Phase Commands**, and then select **Properties** from the pop-up menu. The **Phase Commands Properties** dialog box opens.



2. Configure policy Confirm settings:

- Scroll down to the **BatchView and ActiveX - Phase Commands - Confirmations** policy settings. Select the policy setting and click the corresponding dropdown list. Select **True** to require a user to log on with a user name and password each time the command button is clicked. Select **False** if no logon is required.



In the example shown above, the Clear Failure - Confirm is set to **True**. This will require a user to enter their FactoryTalk user name and password when he or she wants to clear a failure while a batch is running.

- Click **OK** to return to the FactoryTalk Administration Console window.

Tip: Restart all open FactoryTalk Batch components to update changes made in the FactoryTalk Directory.

Configure Equipment Editor and Recipe Editor security

Security for the FactoryTalk Batch Equipment Editor and Recipe Editor is implemented using the FactoryTalk Security product policies defined in the FactoryTalk Directory. Only FactoryTalk users are allowed access to the editors. (See *"FactoryTalk Batch Default Policy Settings"* in the *FactoryTalk Batch Administrator's Guide* for more information.)

There are two levels of security used to support the FactoryTalk Batch Equipment Editor and Recipe Editor: **View Only** and **Full Edit**. See [Configure Access Mode security](#) on [page 218](#) for more information.

Additionally, there are **Configuration Options** product policies created in the Local Directory for the editors. See [Modifying the Equipment Editor configuration options](#) on [page 219](#) for more information.

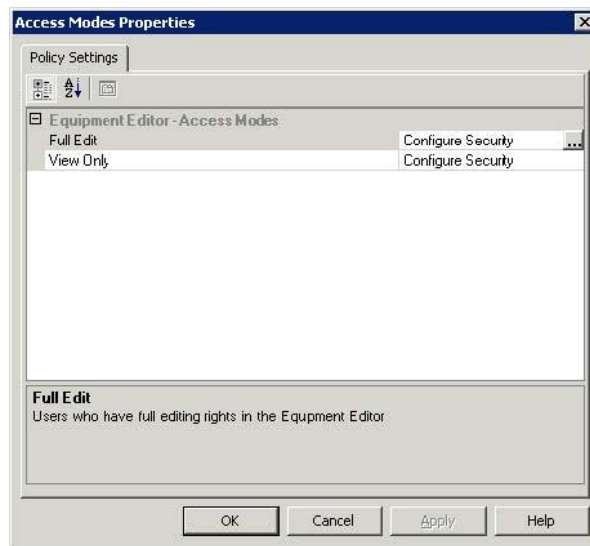
In addition to FactoryTalk Security, you can configure Windows security on the FactoryTalk Batch Equipment Editor and Recipe Editor files and folders in Windows Explorer. (See *"Setting Security on Folders or Files"* in the *FactoryTalk Batch Administrator's Guide* for more information.) If you are

using RDB recipes that are stored in SQL Server, RDB security can also be configured.

Configure Access Mode security

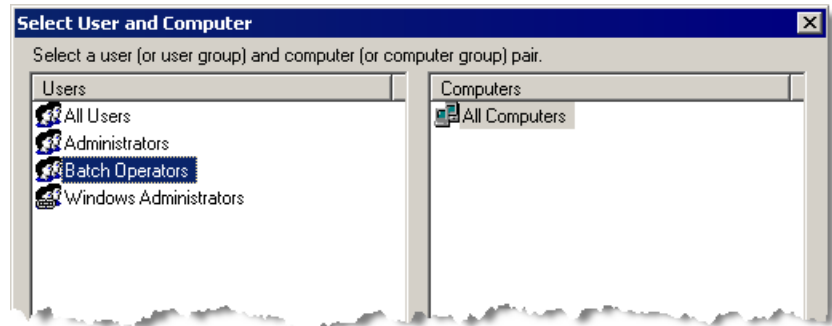
There are two levels of security used to access the FactoryTalk Batch Equipment Editor and Recipe Editor: **View Only** and **Full Edit**.

1. Configure the FactoryTalk Batch Equipment Editor or Recipe Editor Access Modes:
 - Open the FactoryTalk Administration Console and log on to the appropriate FactoryTalk Directory. This example uses the **Network Directory**.
 - Expand **System > Policies > Product Policies > Batch > Equipment Editor** (or Recipe Editor), right-click on **Access Modes**, and then select **Properties** from the pop-up menu.



- From the **Access Modes Properties** dialog box, select the policy setting you want to configure and click the browse button. The **Configure Securable Action** dialog box opens.
2. Tighten security for this feature:
 - Select the **All Users** group and click **Remove**.
 3. Add users or groups:

- To add a user or group select **Add**. The **Select User and Computer** dialog box opens.



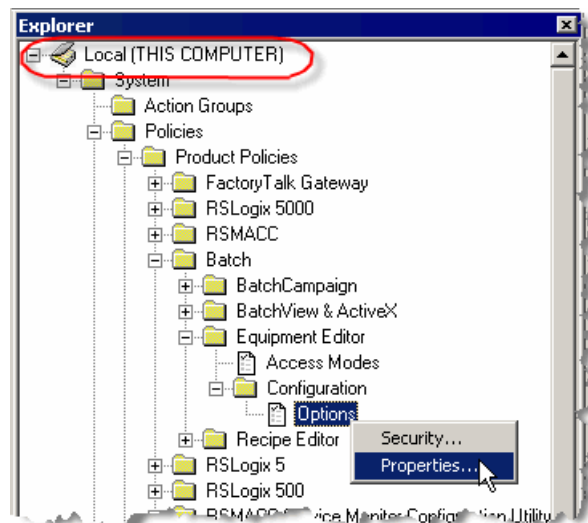
- Select the user or group you want to add and click **OK**. For this example, select **Batch Operators**.
- Click **OK** to close the **Configure Securable Action** dialog box.

Tip: Restart all open FactoryTalk Batch components to update changes made in the FactoryTalk Directory.

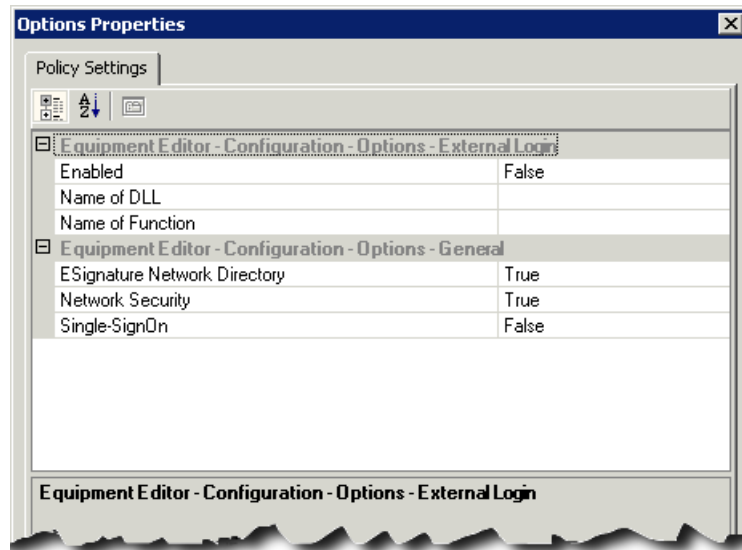
Modifying the Equipment Editor configuration options

The following instructions are specific to the FactoryTalk Batch Equipment Editor. The FactoryTalk Batch Recipe Editor configuration options are configured similarly.

- Open the FactoryTalk Administration Console. Log on to the FactoryTalk **Local Directory**.

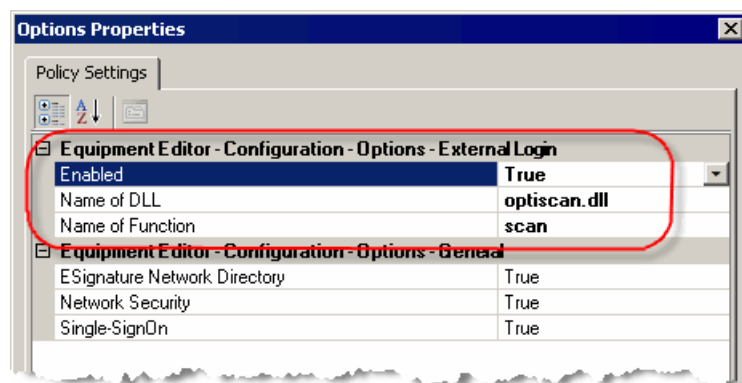


- Expand **System > Policies > Product Policies > Batch > Equipment Editor** (or Recipe Editor) > **Configuration**, right-click on **Options**, and then select **Properties** from the pop-up menu.



- From the **Options Properties** dialog box, make the necessary policy setting changes.

For example, the FactoryTalk Batch Equipment Editor and Recipe Editor allow you to use an external security device, such as a retinal scanner. If you want to enable security for the external device, you would configure the External Login settings as shown in the example below.



(See "Using an External Security Device" in the FactoryTalk Batch Administrator's Guide for more information.)

- Click **OK** to save the configuration changes and return to FactoryTalk Administration Console.

Tip: Restart all open FactoryTalk Batch components to update changes made in the FactoryTalk Directory.

Where to go from here

Do one of the following:

- Continue assigning permissions for FactoryTalk Batch client actions and commands, if desired.
- Go to [RSLinx and FactoryTalk Security](#) on [page 113](#) to learn how to use FactoryTalk Security with RSLinx software.
- Go to [Logix Designer application and FactoryTalk Security](#) on [page 125](#) to learn how to use FactoryTalk Security with Logix Designer application to secure projects and devices like Logix5000, PLC, and SLC controllers.
- Go to [FactoryTalk View SE and FactoryTalk Security](#) on [page 151](#) to learn how to use FactoryTalk Security with FactoryTalk View SE.
- Go to [FactoryTalk View ME and FactoryTalk Security](#) on [page 175](#) to learn how to use FactoryTalk Security with FactoryTalk View ME.
- Go to [Deploying a FactoryTalk system](#) on [page 223](#) to learn about deploying a FactoryTalk system to runtime computers.

Deploying a FactoryTalk system

This section gives a high-level look at a scenario for moving a FactoryTalk system that was built on an offline development system to an online runtime system.

Assumptions

The scenario in this section is based on the following assumptions:

- C: is the system drive on each of the computers
- The FactoryTalk Services Platform is installed and configured on all computers in both the development network and runtime network. See [On the runtime system computers](#) on [page 226](#).
- FactoryTalk View SE is installed, activated, and configured
- One computer on the network has been identified as a FactoryTalk Network Directory Server, and all of the other participating computers on the network have been configured as clients, pointing to that Network Directory Server computer

Be sure to uninstall previous versions of Rockwell Software products before installing new versions. In addition, be sure to install compatible versions of the FactoryTalk Services Platform and Rockwell Software products.

Setting up the development system computers

Follow the steps below on the appropriate development system computers to prepare to move a FactoryTalk system from a development network to a runtime network.

Step 1: On a Network Directory computer

From any computer in the Network Directory, run the FactoryTalk Administration Console and back up the entire FactoryTalk Network Directory.

When you back up an entire FactoryTalk Network Directory, the resulting *.bak* file includes all of the applications in that directory and all of the settings in the System folder.



Restoring the System folder overwrites all user and computer accounts and groups, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory. Use with caution.

The Backup tool creates a backup file that contains:

- the application name
- the area definitions
- the HMI Server name and location (in which area and on which computer)
- the data server names, type and location (in which area and on which computer)
- FactoryTalk Alarms and Events server configuration, including Tag Alarm and Event server alarm definitions.

For details, see *Back up an entire FactoryTalk Directory* and *Choosing the correct backup and restore options* in the FactoryTalk Help.

Move the backup file (*.BAK) from the development computer to the runtime FactoryTalk Network Directory computer. The .bak file is located in **C:\Users\Public\Documents**.

Step 2: On the FactoryTalk View Site Edition Server computer

Move the HMI project files from the development computer to the appropriate View SE runtime computers. Copy the entire folder containing the HMI Server files. This folder has the same name as the HMI Server name and is located in **C:\Documents and Settings\All**

Users\Documents\RSView Enterprise\SE\HMI Projects. This copy is not possible if the HMI Server is running. See *FactoryTalk View Site Edition* documentation for more detailed help on backing up your HMI Servers.

Important: You can use the HMI Backup and Restore utility to backup a loaded HMI Server. See Answer ID 30310 in the Rockwell Knowledgebase:
http://rockwellautomation.custhelp.com/cgi-bin/rockwellautomation.cfg/php/enduser/std_adp.php?p_faqid=30310

Step 3: On the FactoryTalk View Studio computer

Move the client configuration files (*.cli) from the development computer to the runtime View SE Client computers. The location on the runtime computer is not important, but by default, the client files are located in

C:\Documents and Settings\All Users\Documents\RSView Enterprise\SE\Client. See FactoryTalk View Studio documentation for additional help.

Step 4: On the RSLinx Classic or RSLinx Enterprise computer

- **RSLinx Enterprise servers** — copy the communications configuration file, *RSLinxNG.xml*, from the directory location: **C:\Documents and Settings\All Users\Application Data\Rockwell\RSLinx Enterprise\RSLinxNG.xml**.

For RSLinx Enterprise, the device shortcuts are backed up automatically as part of backing up entire Network Directory in [Step 1 On a Network Directory computer](#) on [page 226](#) above.

- **RSLinx Classic data servers** — run the RSLinx Backup Restore Utility. From the Windows **Start** menu, select **All Programs > Rockwell Software > RSLinx > Backup Restore Utility**.

Step 5: On the Microsoft SQL Server computer

If your FactoryTalk system includes Microsoft SQL Server databases for logging historical data, including FactoryTalk Alarms and Events logs, back up any data you want to deploy to another system.

Step 6: On the FactoryTalk Transaction Manager computer

If your FactoryTalk system includes FactoryTalk Transaction Manager, back up your project. From the **Configuration** menu, select **Backup**.

Step 7: On the FactoryTalk Batch Server computer

If your FactoryTalk system includes FactoryTalk Batch, use the Batch Service Manager to stop the Batch Server. Back up Batch Server and client files. For help, see the FactoryTalk Batch Installation Guide.

Step 8: On the FactoryTalk Batch client computers

If your FactoryTalk system includes FactoryTalk Batch, back up Batch client files. For help, see the FactoryTalk Batch Installation Guide.

On the runtime system computers

Install and activate Rockwell Software products on the appropriate runtime computers. As part of installing each product, also install FactoryTalk Services Platform.

In addition, on each FactoryTalk Network Directory client computer, specify which computer on the network is hosting the FactoryTalk Network Directory Server. Then follow the steps below.

Step 1: On a Network Directory computer

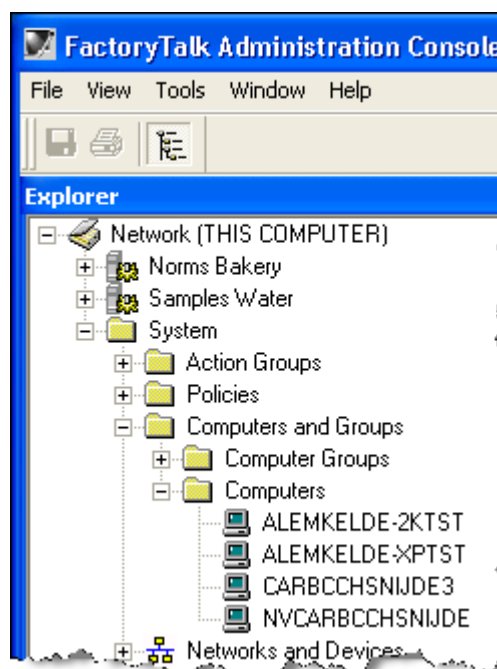
Before you begin, shut down all Rockwell Software products running on every computer on the network.

Next, on any computer in the Network Directory, run the FactoryTalk Administration Console and restore the directory you backed up previously. See [Restore a FactoryTalk Directory](#) on [page 233](#).

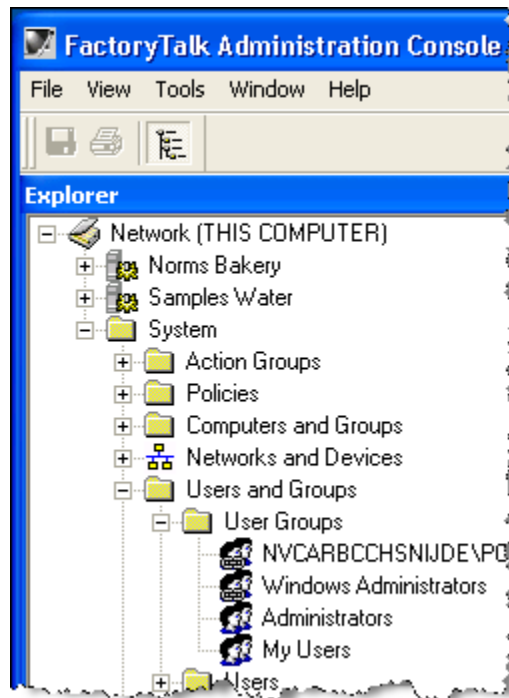
If necessary, do the following:

- If the computers in your runtime system are on the same physical network as your development computers but are in a different domain, then rename any computers with the same name. A Windows Domain Controller will not allow multiple computers in different domains to have the same name on the same network.

(In the Explorer window, expand the **Computers and Groups** folder, expand the Computers folder, right-click the computer account icon, and then click **Properties** on the pop-up menu. Type the new name for the computer, and then click **OK**.)



- If you created Windows-linked user accounts on your development system, recreate all security settings for these accounts in your runtime system.
- If you created Windows-linked user groups on your development system, move them to the new domain.



(In the Explorer window, expand the **Users and Groups** folder, expand the **User Groups** folder, right-click the user group you want to move to the new domain, and then click **Properties** on the pop-up menu. In the **Properties** dialog box, click **Change Domain**, and then choose the new domain. The new domain must already contain a user group of the same name.) Click **OK** to save.

Step 2: On the FactoryTalk View Site Edition Server computer

Restore the HMI project and identify the location of data servers. Open FactoryTalk View Studio (or the View Administration Console), and edit the application. The HMI and data servers will be in error because they are still configured for the development computer. Edit the properties of the HMI and data servers to reflect their new location. See FactoryTalk View documentation for help.

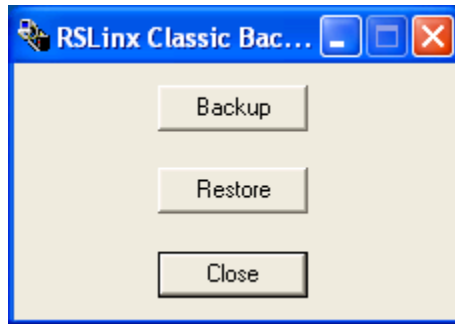
Important: Make sure that the folder name and HMI project file name (*.sed) have the same name or the HMI Server will not load properly.

Step 3: On the FactoryTalk View Site Edition Client computers

Restore client configuration files (*.cli). The location on the runtime computer is not important, but by default, the client files are located in **C:\Documents and Settings\All Users\Documents\RSView Enterprise\SE\Client**. See FactoryTalk View documentation for help.

Step 4: On the RSLinx Classic computer

1. Run the RSLinx Backup Restore Utility to restore the RSLinx Classic configuration. From the Windows **Start** menu, point to **All Programs > Rockwell Software > RSLinx > Backup Restore Utility**.

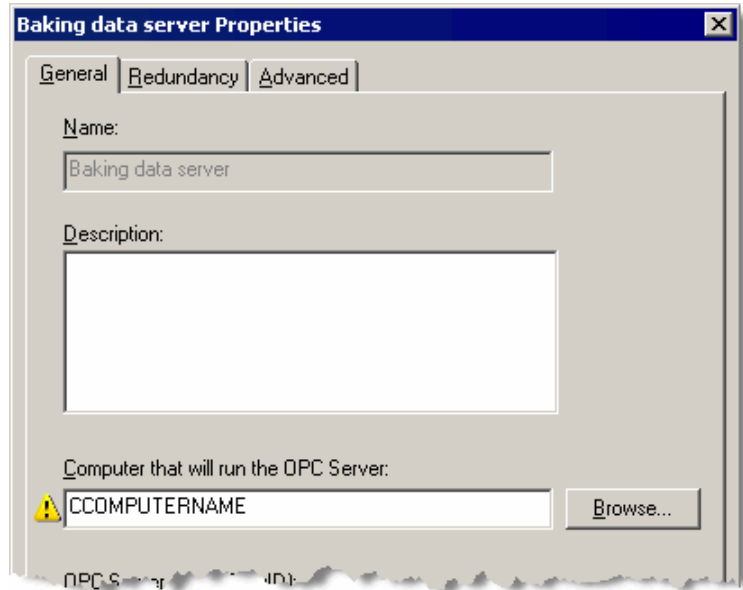


2. Update any offline topics in the project to online topics.
3. To see PLC or SLC symbol files when browsing offline, copy the processor project from the development computer to the runtime computer. Then define the new location of the project file in the RSLinx Classic topic for that processor.

Step 5: On the RSLinx Enterprise server computer

1. Copy the communications configuration file you copied previously back to the same directory location **C:\Documents and Settings\All Users\Application Data\Rockwell\RSLinx Enterprise\RSLinxNG.XML**, and then restart your computer.
2. On any computer in the Network Directory, run FactoryTalk Administration Console.

3. Change the name of the computer hosting the RSLinx Enterprise data servers.
 - Right-click the Data Server icon and then click **Properties** to open the **Data Server Properties** dialog box. In the **Computer hosting the RSLinx Enterprise server** box, identify the name of the runtime computer where the data server is now located. Repeat this step for each defined data server.



Important: You must also update the names of the computers hosting the HMI servers and the Tag Alarms and Events servers.

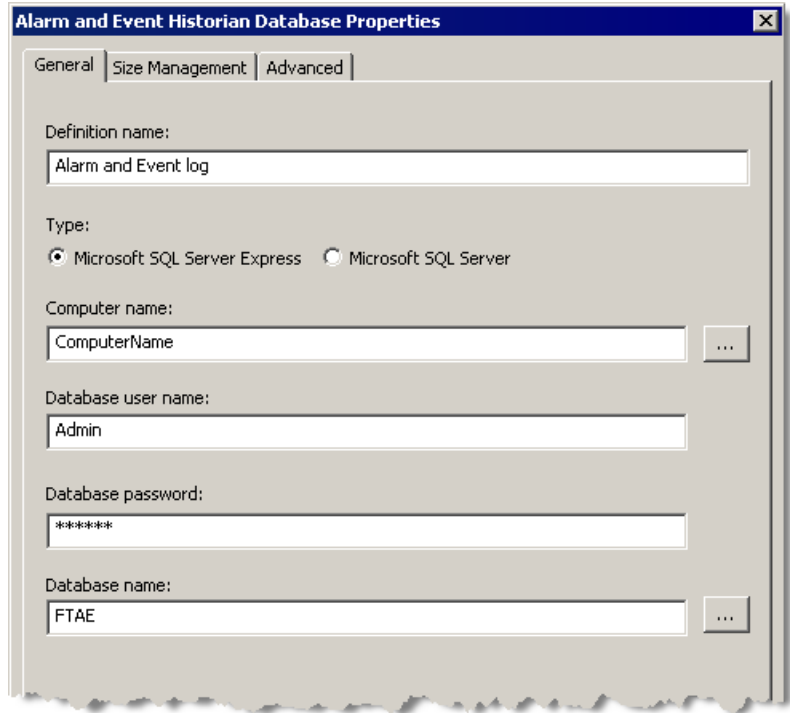
4. Re-map any device shortcuts to their corresponding physical devices listed in the **Communication Setup** editor. For help, see RSLinx Enterprise online help.

Step 6: On the Microsoft SQL Server computer

If your FactoryTalk system includes Microsoft SQL Server databases for logging historical data, including FactoryTalk Alarms and Events logs, restore any data you want to deploy to the new system, and then re-establish a connection between a database definition, held in the directory, and its associated Microsoft SQL Server database.

1. On any computer in the Network Directory, run FactoryTalk Administration Console.
2. From the Explorer window, open **System > Connections > Databases**.

3. Double-click the database definition to open its properties, change the name of the computer hosting the Microsoft SQL Server, and then click **OK**.



The system checks for database tables and creates them, if they do not exist.

Step 7: On the FactoryTalk Transaction Manager computer

If your FactoryTalk system includes FactoryTalk Transaction Manager:

1. Run Transaction Manager and restore the project you backed up. On the **Configuration** menu, click **Restore**.
2. Next change the name of the computer associated with each connector configuration. For each defined Connector Service, right-click the **Configuration name** and select **Define Connector** from the pop-up menu. Change the Host Name from the name of the development computer to the name of the runtime FactoryTalk Transaction Manager computer.

Step 8: On the FactoryTalk Batch Server computer

If your FactoryTalk system includes FactoryTalk Batch, restore FactoryTalk Batch Server and client files. For help, see FactoryTalk Batch Installation Guide.

Step 9: On the FactoryTalk Batch client computers

If your FactoryTalk system includes FactoryTalk Batch, restore FactoryTalk Batch client files. For help, see FactoryTalk Batch Installation Guide.

Backing up an entire FactoryTalk Directory



Restoring the System folder overwrites all user and computer accounts and groups, passwords, policy settings, and security settings for all applications in the FactoryTalk Directory. Use with caution.

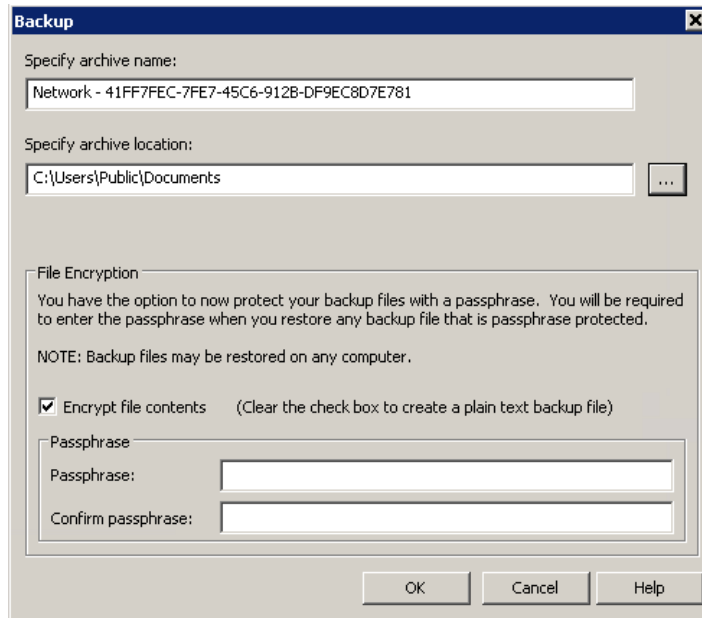
Required security permissions

A system-wide security policy, called User Rights Assignment, determines who has permission to perform backup and restore operations. From FactoryTalk Administration Console or FactoryTalk View Studio Explorer window, open **System > Policies > System Policies**, and then double-click **User Rights Assignment**.

To back up a FactoryTalk Directory:

1. At the top of the FactoryTalk Administration Console Explorer window, right-click the Network or Local Directory icon.
2. From the pop-up menu, select **Backup**.

3. Use the default name or type another name for the backup file. It is recommended that you do not change the default archive name. The default name contains the security authority identifier which allows you to easily identify the archive file associated with a specific directory.



Tip: The security authority identifier is a unique ID generated for each FactoryTalk Directory scope object to differentiate one directory from another when you install FactoryTalk Services Platform 2.50 or later. The value is represented as a 32-character hexadecimal string, such as BCC21891-C103-4950-BC5C-C34295D1AE2D. By using this identifier a ControlLogix controller or project can be bound to a specific instance of FactoryTalk Directory. You can modify the identifier in the Modify Security Authority Identifier dialog box. Once a new identifier is generated, you will no longer be able to open the controller or project bound to the old identifier. We recommend that you back up your directory and remove the old bindings from all controllers and controller projects before proceeding. For more information, refer to FactoryTalk Help.

4. Use the default archive location or click the **Browse** button, and then select a location for the backup file. Click **OK** to close the **Browse for Folder** dialog box.
5. To encrypt your archive file, select the **Encrypt file contents** check box, and then enter the same passphrase in the **Passphrase** and **Confirm passphrase** fields. If you clear this check box, your backup file will not be encrypted or protected.

The **Encrypt file contents** check box will not be available if the version of your operating system does not support the proper level of encryption. For more information, see "Back up FactoryTalk Directory, System folder, or applications" in the FactoryTalk Help. In the **Backup** window, click **OK**.

Important: Remember the passphrase if you choose to encrypt your file contents. The archive file cannot be restored without the correct passphrase.

Unless you specified a different file name, FactoryTalk Administration Console creates a directory backup file with its current security authority identifier in the default location or in the location you specified. If a backup file with the same name already exists in the location you've chosen, the system asks whether you want to overwrite the existing file.

6. After backing up a directory, back up and restore project files and databases separately from individual software products that are participating in the FactoryTalk system. See "After backing up a directory or application" in the FactoryTalk Help.

To deploy a FactoryTalk system from one computer to another, restore a FactoryTalk Directory backup archive.

Restore a FactoryTalk Directory

Important: Do not restore an archive file created under FactoryTalk Services Platform 2.10 (CPR 9) or later into a FactoryTalk Directory that is currently running FactoryTalk Automation Platform 2.00 (CPR 7). This restore scenario is not supported and may have unexpected results.

A FactoryTalk Directory archive file that is automatically created when you install or upgrade FactoryTalk Services Platform 2.50 or later can only be restored on the same computer.

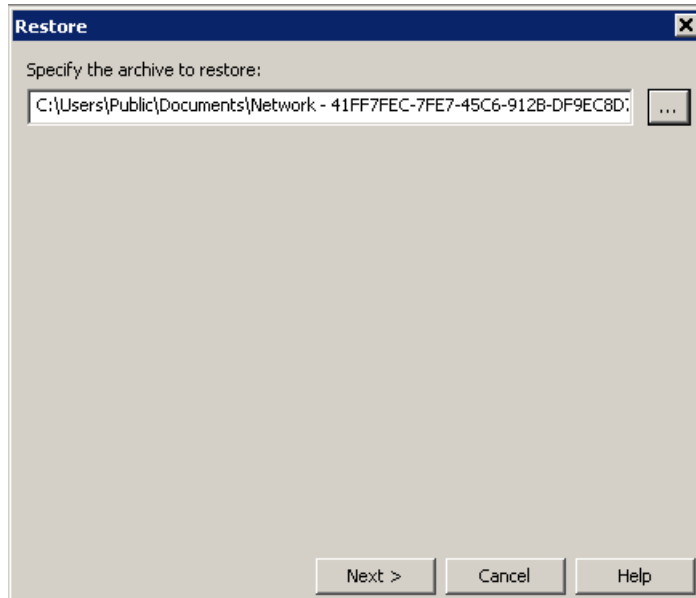
Required security permissions

A system-wide security policy, called User Rights Assignment, determines who has permission to perform backup and restore operations. From FactoryTalk Administration Console or FactoryTalk View Studio Explorer window, open **System > Policies > System Policies**, and then double-click **User Rights Assignment**.

To restore a FactoryTalk Directory:

1. Ensure that the applications, located in the FactoryTalk Directory that you are restoring into, are not currently expanded in the Explorer window or being used by some other product or component. If applications are currently in use, the restore will fail.

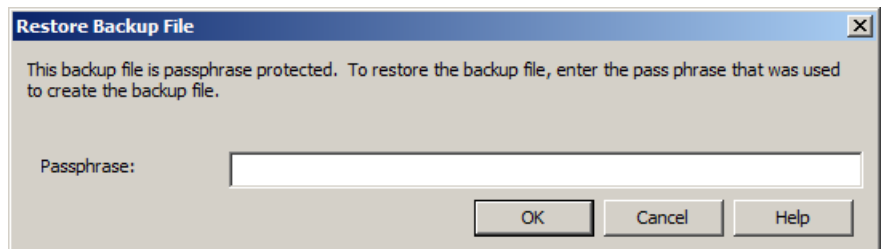
2. In the FactoryTalk Administration Console Explorer window, right-click the **Network** or **Local** icon. From the pop-up menu, click **Restore**.



3. In the **Restore** dialog box, click the **Browse** button, select the backup file you want to restore, and then click **Open**. To continue, click **Next**.

By default, a backup file for a Network Directory or Local Directory is named with its current security authority identifier, for example, **Network - 72CE2C2E-5175-4C26-98AE-3ABE5AC7F8EC.bak** or **Local - C565C77A-4664-4E6C-9779-1EC729B3A8A0.bak**.

4. If the backup file is encrypted, the **Restore Backup File** dialog box is displayed. Enter the passphrase that was used during the backup operation.





An error message opens if the passphrase you entered is not correct. Enter the passphrase again. If the wrong passphrase is entered three times, the **Restore Backup File** dialog box closes. Select the archive and try again.

5. After you enter the correct passphrase, the **Restore** dialog box shows the type of archive you are restoring and what applications are contained in the archive. You cannot select individual applications.

By default, the entire FactoryTalk Directory will be restored. The restore options show when you perform the restore operation from the **Modify Security Authority Identifier** dialog box.

Restore

Archive name:

Network - 41FF7FEC-7FE7-45C6-912B-DF9EC8D7E781

Directory ID:

41FF7FEC-7FE7-45C6-912B-DF9EC8D7E781

Archive type:

FactoryTalk Directory (all applications, accounts, passwords, policies and security settings)

Application(s):

InstantFizz

Samples Water

☒ Restore directory contents only

☐ Restore security authority identifier only

< Back

Finish

Cancel

Help

Select the desired option to restore the backup file:

To restore...	Select this option...
the FactoryTalk Directory contents, including all applications, all user and computer accounts and groups, passwords, policy settings, and security settings.	Restore directory contents only
the security authority identifier only (for example, when you want to access a controller without restoring your directory contents).	Restore security authority identifier only

6. To restore the FactoryTalk Directory contained in the selected archive, click **Finish**.

If you restore an archive created in an earlier version of the FactoryTalk platform into a later version, the restore process automatically updates the data in the System folder to be compatible with the later version, while retaining the original data from the archive.

For example, suppose you restore an archive created under FactoryTalk Automation Platform 2.00 (CPR 7) into a FactoryTalk Directory that has been upgraded to FactoryTalk Services Platform 2.10 (CPR 9) or later. The restore process retains the original user accounts and all system-wide security and policy settings, but also updates the System folder to include new options and policies available with FactoryTalk Services Platform 2.10 or later.

7. After restoring a FactoryTalk Directory, back up and restore project files and databases from your individual software products, and then verify security and computer accounts. See below.

After restoring a FactoryTalk Directory

A backup archive does not include configuration and project information specific to particular software products. Back up and restore project files from individual software products separately. See "After backing up a directory or application" in the FactoryTalk Help.

- If restoring an entire FactoryTalk Directory, see [After restoring an entire FactoryTalk Directory](#) on [page 236](#).
- If restoring the FactoryTalk Directory contents only, see [After restoring the FactoryTalk Directory contents](#) on [page 238](#).
- If restoring restoring the FactoryTalk Directory security authority identifier only, see [After restoring the FactoryTalk Directory security authority identifier](#) on [page 239](#).

After restoring an entire FactoryTalk Directory

If your applications include:

- **HMI servers**, restore FactoryTalk View files separately. See FactoryTalk View documentation for help.
- **RSLinx Classic data servers**, see [Step 4 On the RSLinx Classic computer](#) on [page 228](#).
- **RSLinx Enterprise servers**, see [Step 5 On the RSLinx Enterprise server computer](#) on [page 228](#).
- **FactoryTalk Alarms and Events Logs**, see [Step 6 On the Microsoft SQL Server computer](#) on [page 229](#).
- **FactoryTalk Transaction Manager**, see [Step 7 On the FactoryTalk Transaction Manager computer](#) on [page 230](#).
- **FactoryTalk Batch**, copy the FactoryTalk Batch files you copied previously back to the same directory locations. See FactoryTalk Batch documentation for help.

After restoring an entire FactoryTalk Directory, the old security authority identifier is also replaced with the identifier from the backup archive.

Perform the following actions:

- **Update Windows-linked groups.** When the System folder is deployed to a new Windows domain, Windows-linked user groups that existed in the original domain may no longer exist in the new domain. An administrator can use the FactoryTalk Administration Console to change the original Windows-linked groups to groups that exist in the new domain. Security settings that refer to the Windows-linked groups in the new domain then update automatically. See "Move Windows-linked user accounts to a different domain" in FactoryTalk Help.

If your system used local workstation accounts as part of a Windows workgroup, Windows-linked user accounts will be missing their security settings after the System folder is restored. We strongly recommend using FactoryTalk Security accounts, instead of Windows-linked accounts, with workgroups. See "Windows-linked accounts are missing permissions after restore" in FactoryTalk Help. See also "Using Windows-linked accounts with Windows workgroups" in FactoryTalk Help.

- **Update computer accounts in the Network Directory.** If the system policy "Require computer accounts for all client machines" is enabled, then only client computers that have been added to the list of computers in the Network Directory can access that directory. When a Network Directory is restored, the directory automatically adds the computer on which the Network Directory Server resides, and the client computer from which the restore operation was performed, to the System folder in the Network Directory.
- After restoring a directory in a new domain, update computer accounts to allow the computers on the network access to the Network Directory. To update computer accounts, run FactoryTalk Administration Console on either the Network Directory Server computer or on the client computer where the restore was performed, and log on as an administrator.

- Rename existing computer accounts. Rename existing computer accounts from the old domain to easily map them to computers on the new domain. This retains any security settings that were applied to the computer accounts in the old domain. To rename a computer account, right-click it in the Explorer window, click **Properties** on the pop-up menu, and then either type the name of a computer or click the **Browse** button to search for a computer.
- Delete old computer accounts. Delete computer accounts that no longer exist in the new domain and that do not map to computers in the new domain. To delete a computer account, right-click it in the Explorer window, and then click **Delete** on the context menu.
- Add new computer accounts. Add computer accounts to allow computers on the network access to the restored Network Directory. To add a computer account, right-click the Computers folder in the Explorer window, and then click **New Computer** on the pop-up menu.

If you delete a computer account and then recreate it, its security settings are lost. To map computers from one domain to another, rename the computer accounts rather than deleting and recreating them.

- **Verify security settings for Networks and Devices** and update them if necessary. The Networks and Devices tree shows information about the networks and devices that are connected to the local computer. The contents of the Networks and Devices tree are not included in the backup archive, but any security settings that have been defined for networks and devices are included in the backup archive. If an archive is restored on a computer that is connected to the same networks and devices using the same drivers or logical names, the security settings restored from the archive file will take effect.
- **If you change the name of a computer hosting an alarm server**, the new host computer must be restarted. This is necessary to ensure the alarm servers start up.
- **If the alarm history database has not been restored and was never created on the system**, you must create the alarm log database as follows: In FactoryTalk Administration Console, from the Explorer window, open **System > Connections > Databases**. Double-click the database definition to open its properties. If necessary, update the name of the computer hosting the database server, and then click **OK**. Clicking **OK** creates the alarm log database.

After restoring the FactoryTalk Directory contents

See [After restoring an entire FactoryTalk Directory](#) on [page 236](#).



Restoring the FactoryTalk Directory contents only does not replace the current security authority identifier of your directory.

After restoring the FactoryTalk Directory security authority identifier

Backup your FactoryTalk Directory. The old security authority identifier is replaced with the identifier from the backup file. It is strongly recommended to make a backup of the directory with the new identifier.

Upgrade FactoryTalk Services Platform

This section outlines the steps for upgrading FactoryTalk® Security. It includes instructions for installing the latest version of the FactoryTalk Services Platform, activating the software, and configuring FactoryTalk directories.

The FactoryTalk Services Platform is an integrated part of each FactoryTalk product's install process, although each product might install it differently. With FactoryTalk View, for example, installing the FactoryTalk Services Platform is just one of several installation steps.

Before you begin

FactoryTalk Services Platform installs along with the software products that require it. Installation and upgrade steps vary, depending on which products you are installing or upgrading. For step-by-step instructions, see each product's installation information.

If you are upgrading a client computer to the latest FactoryTalk Services Platform version (for example, 2.70), you may also need to upgrade the computer hosting the FactoryTalk Network Directory Server to FactoryTalk Services Platform version 2.70. In this release, several products added new security policies that will not function correctly if the FactoryTalk Network Directory Server is not upgraded to include them. For additional information on upgrading a previous version of the FactoryTalk Network Directory Server or updates for the other products that may require updates, see Answer ID 49190 in the Rockwell Automation Knowledgebase:

http://rockwellautomation.custhelp.com/cgi-bin/rockwellautomation.cfg/php/enduser/std_adp.php?p_faqid=49190

When upgrading FactoryTalk platform software

When you upgrade to FactoryTalk Services Platform 2.10 (CPR 9) or later on a computer that has previously had FactoryTalk Automation Platform 2.00 (CPR 7) installed, the installation process:

- **creates a backup file** for any existing FactoryTalk Directory already configured on the computer. Should you later need to uninstall FactoryTalk Services Platform and reinstall an earlier version, restore this backup file to return the FactoryTalk Directory to its earlier state.

See Restore an earlier system after upgrading FactoryTalk platform software.

- **checks for both a Local Directory and a Network Directory** on the computer. If a directory is found, the installation process updates it with support for new policies and features, but leaves original security and policy settings unchanged.

If either directory has not been created, the installation process creates it and configures it by automatically adding the local computer account, the local Windows Administrators group, and the local Windows Authenticated Users group to the directory, and by setting a default to grant all new user accounts full access to the directory. This step allows any user account with Windows Administrator privileges to be able to immediately log on to the directory, without first having to create a FactoryTalk Administrator account.

- if necessary, **updates each FactoryTalk Directory** with new product policies, system policies, and support for new features.
- **leaves all original settings unchanged**, including security settings, user accounts and groups, and policy settings.

When upgrading computers in a distributed system

- Upgrade client computers only if the version of the FactoryTalk platform software installed on the FactoryTalk Directory server computer is not compatible with the new versions of the products you are installing. For details about compatible versions of the FactoryTalk platform software, see the documentation provided with your products.
- If you do need to upgrade client computers, we recommend that you upgrade client computers first, then upgrade the server computer hosting the FactoryTalk Directory Server, and finally, upgrade any remaining run-time server computers last.
- When upgrading client computers from FactoryTalk Automation Platform version 2.00 (CPR 7), you must upgrade client computers first, and then upgrade the FactoryTalk Directory server computer last. You cannot connect CPR 7 clients to a CPR 9 or later FactoryTalk Network Directory Server.
- To use the new features available with FactoryTalk Services Platform 2.10 (CPR 9) or later, the FactoryTalk Directory Server computer must be upgraded. Any new features are not supported on a FactoryTalk Directory Server computer that is running an earlier version of the FactoryTalk platform software.
- If the FactoryTalk Network Directory Server computer is upgraded to FactoryTalk Services Platform 2.10 (CPR 9) or later, then the products

installed on all client computers on the network must also be upgraded to compatible versions. For details, see the documentation supplied with your products.

To upgrade client computers:

1. Before upgrading to FactoryTalk Services Platform, shut down all Rockwell Automation software products running on the computer.
2. Ensure you are logged on with Windows Administrator rights.

As part of the installation process, FactoryTalk Services Platform creates program folders and modifies registry entries, and installs the FactoryTalk services to the computer. To make these modifications, the currently logged-on user must have administrative rights in Windows, on the computer where FactoryTalk Services Platform is installed.

To upgrade server computers:

1. Log on to Windows with Administrator rights.
2. Before upgrading FactoryTalk Services Platform, all related services running on the computer are automatically shut down. To avoid loss of data, shut down all Rockwell Automation software products running on the computer before beginning the upgrade.
3. Before upgrading a server computer, disconnect the computer from the network. This prevents client computers from accessing the server during the upgrade. If you are running FactoryTalk server products on your computer and you cannot disconnect the computer from the network, uninstall the server products before upgrading FactoryTalk Services Platform on the computer.
4. If you are upgrading the FactoryTalk Network Directory Server computer, you must disconnect the computer from the network before performing the upgrade.
5. Some Rockwell Automation software products run as services in the background. Before upgrading to FactoryTalk Services Platform, you might need to uninstall those products. For details, see the documentation for your product.
6. When the upgrade is complete, reconnect the server computer to the network.

Identifying the installed version of the FactoryTalk platform

1. On the Windows **Start** menu, click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. In the list of installed programs, either FactoryTalk Automation Platform or FactoryTalk Services Platform appears, with the version number shown beside it.

What you need

- The installation disc of a FactoryTalk-enabled product
- Access to the Internet (to activate your software)

Tip: For discussion purposes, this guide uses the FactoryTalk View installation disc to install the applications discussed in the following sections of this guide. You will install FactoryTalk Services Platform, FactoryTalk Activation, and FactoryTalk View SE from this CD.

Installing FactoryTalk Services Platform

When you install FactoryTalk Services Platform, the installation process creates a backup file of any existing FactoryTalk Directories already configured on the computer. Should you later need to uninstall FactoryTalk Services Platform and reinstall a previous version, restore this backup file to return the FactoryTalk Directory to its earlier state.

Tip: With version 2.10 (CPR 9), FactoryTalk Automation Platform was renamed FactoryTalk Services Platform.

Along with the FactoryTalk Services, FactoryTalk Services Platform installs the following security-related components:

- **Import RSSecurity Configuration** – for migrating an entire RSSecurity Server system to FactoryTalk Security. For more information, see "If required, import an RSSecurity Server database by following the steps below:" on page 197.
- **RSSecurity Emulator Install** – for connecting existing RSSecurity Server clients to the FactoryTalk Directory or for using RSLinx Enterprise and Logix Designer application with FactoryTalk Security. For more information, [Install the Rockwell Software Security Emulator on page 114](#).

Tip: FactoryTalk Security replaced RSAssetSecurity in CPR 9.

To Install FactoryTalk Services Platform:

- a. Insert your FactoryTalk product disc, like FactoryTalk View, and wait for the Setup program to begin.

If Setup does not start automatically, run **D:\setup.exe** where D is the drive containing the disc.

- b. In the FactoryTalk View Setup window, select **Stand-alone FactoryTalk Directory Server** and click **Next**.

Important: During the installation, if the setup program detects an earlier version of FactoryTalk Services Platform, it prompts you to uninstall it first. The setup program will do this for you if you click **Yes** at this prompt.

- c. Follow the prompts to complete the FactoryTalk Services Platform install.

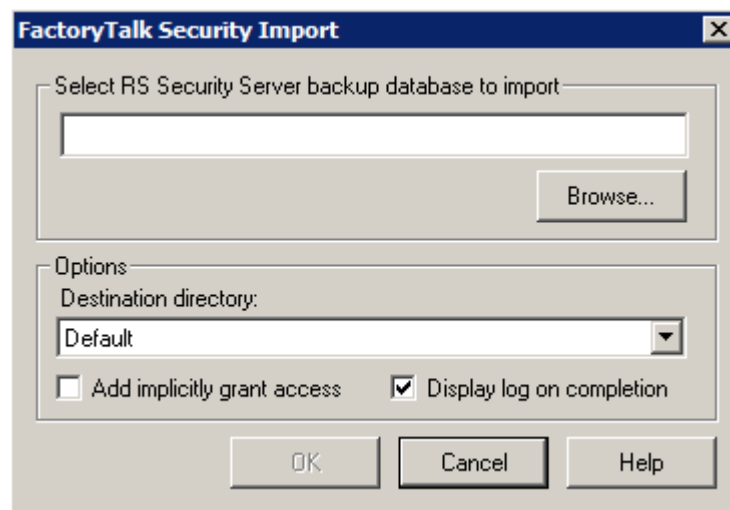
The setup program backs up the existing FactoryTalk Directories and notifies you of the location of the back up files.

After FactoryTalk Services Platform is installed, do one of the following and log on to the FactoryTalk Network Directory:

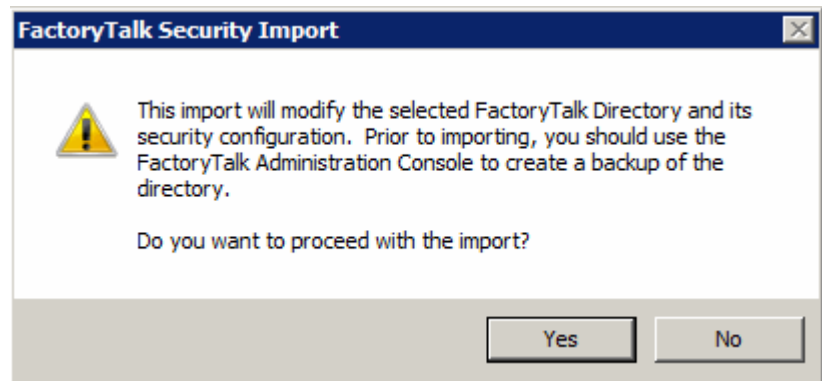
- a. On the Windows Start menu, click **Start > All Programs > Rockwell Software > FactoryTalk Tools > Log on to FactoryTalk**.
- b. Log on to a FactoryTalk product and use the same credentials to also automatically log on to the FactoryTalk Directory.

If required, import an RS Security Server database by following the steps below:

- a. From the Start menu, select **All Programs > Rockwell Software > FactoryTalk Tools > Import RS Security Configuration**.
- b. In the **FactoryTalk Security Import** dialog, select the import file and destination directory and click **OK**.



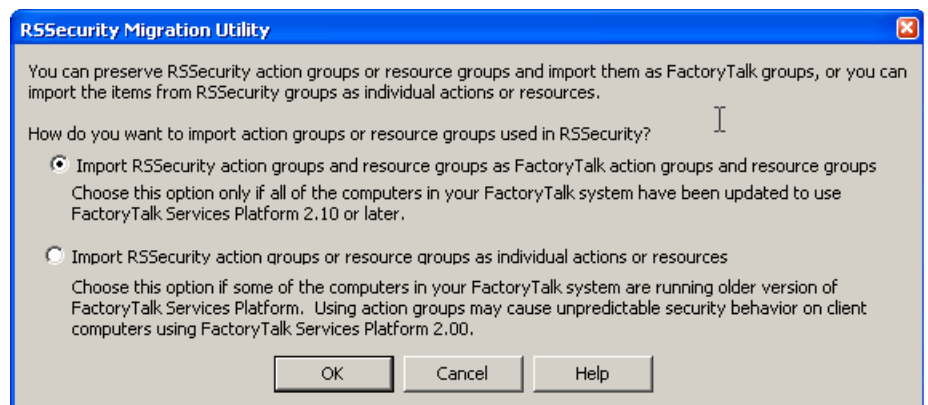
- c. Click **Yes** at the Warning message.



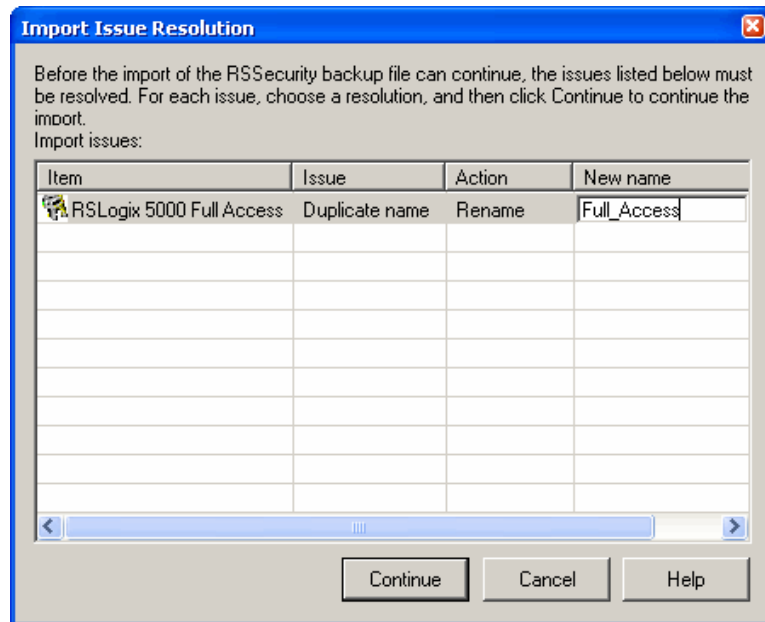
- d. If prompted to log on to FactoryTalk, enter your FactoryTalk user name and password and then click **OK**. The import status appears.



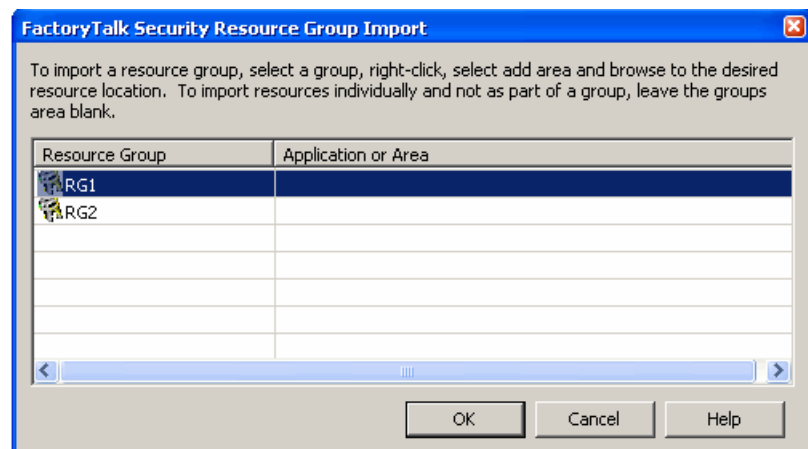
- e. Select how you want action and resource groups to be imported into FactoryTalk and click **OK**.



- f. Review the import issue resolution and click **Continue**.

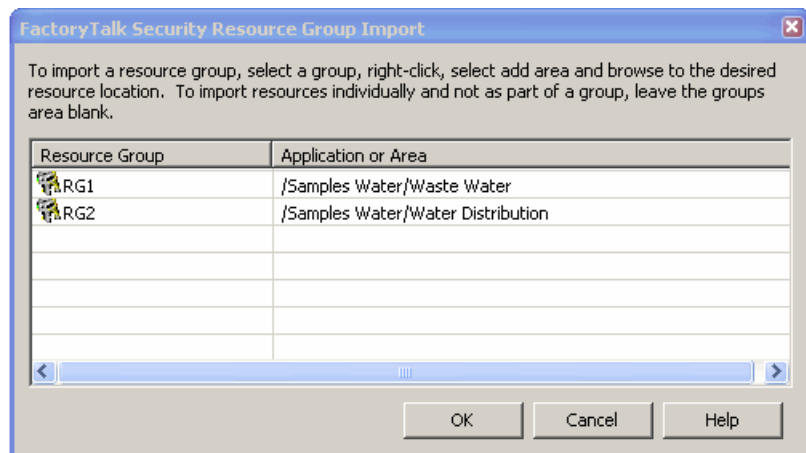


- g. Select a group to import.



- h. Right-click the selected group, select **Add Area** and browse to the resource location.

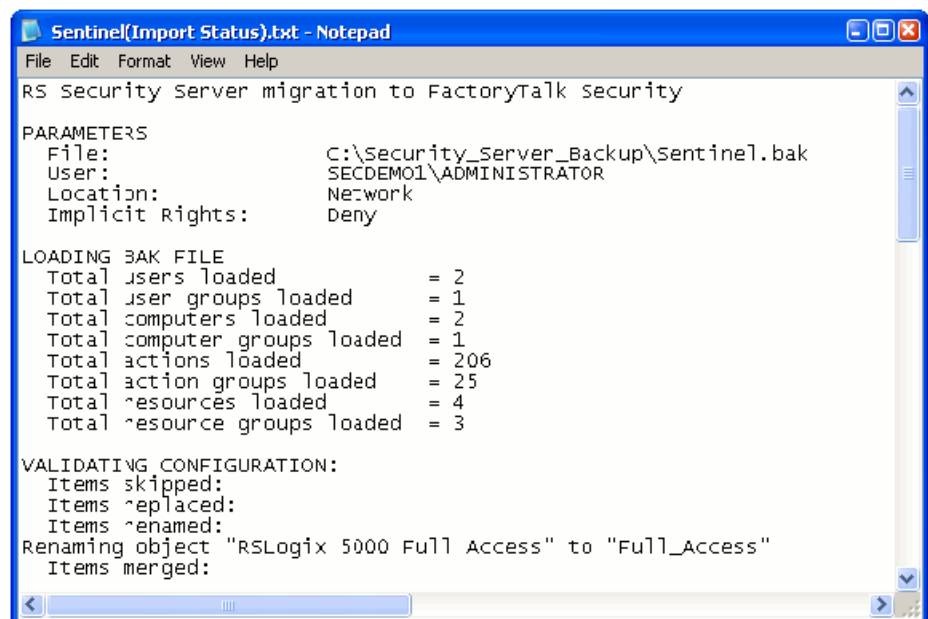
The image below shows that the resource groups RG1 and RG2 were mapped to existing FactoryTalk applications:



- i. Click **OK** to complete the import, and then click **OK** on the "Import successful" message.

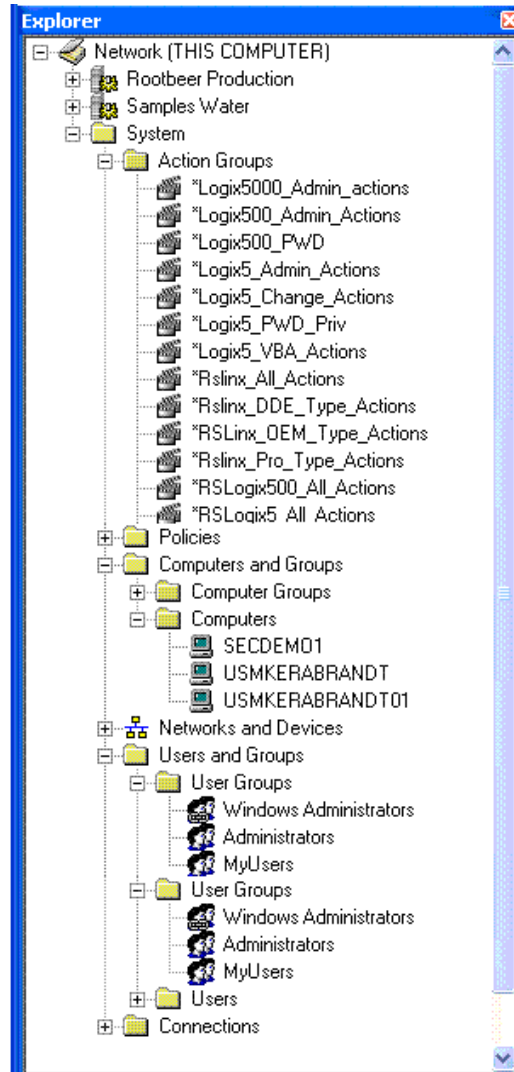
Import Status Text File

This graphic shows an example of the Import Status text file that is created when an import is completed.



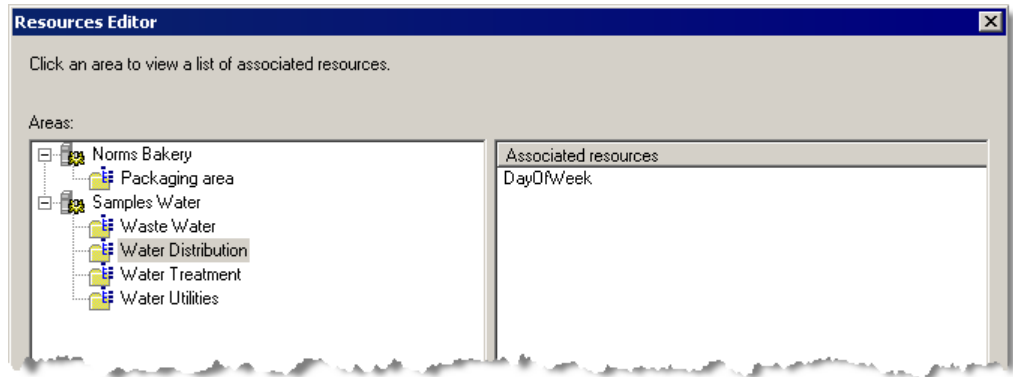
Organizer Import Result

This graphic shows the results of the import process in the Organizer.



Resource Editor

This graphic shows the results of the import in the Resource Editor.



Install FactoryTalk Web Services

FactoryTalk Web Services allow web-enabled Rockwell Automation software products to access FactoryTalk services over a network using the Hypertext Transfer Protocol (HTTP) or the Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). Introduced in this release, the **FactoryTalk Security Web Service** is the first of these Web services.

The FactoryTalk Security Web Service allows clients to interact with the FactoryTalk Directory for authentication and authorization. The Web service also provides support for Rockwell Automation Software products running in environments such as Linux and Java. To use the Web Service, you must install Internet Information Services (IIS) on the computer hosting the FactoryTalk Directory.

For details about installing FactoryTalk Web Services, see the instructions in this chapter. For details about using FactoryTalk Web Services with your FactoryTalk-enabled product, see your product documentation.

Note: If you are deploying the Web services in an environment where privacy of the network communications can be at risk, we recommend that you configure your Web server to support only the encrypted HTTPS protocol. For details, see the administrator documentation supplied with the version of IIS you are using.

Install Microsoft Internet Information Services

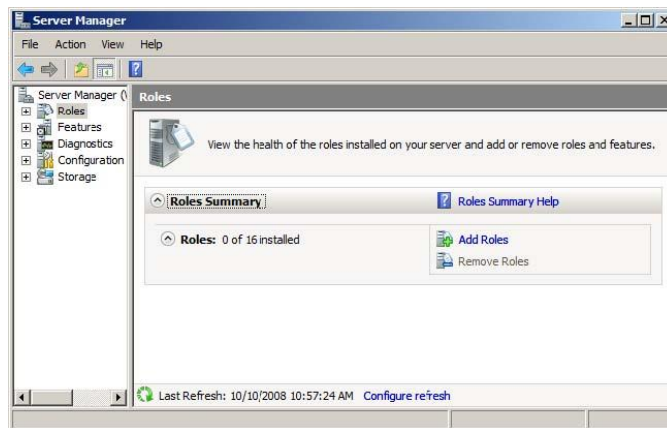
The steps to install Internet Information Services are slightly different for:

- Windows Server 2008 or Windows Server 2012
- Windows 7, Windows 8, or Windows 8.1

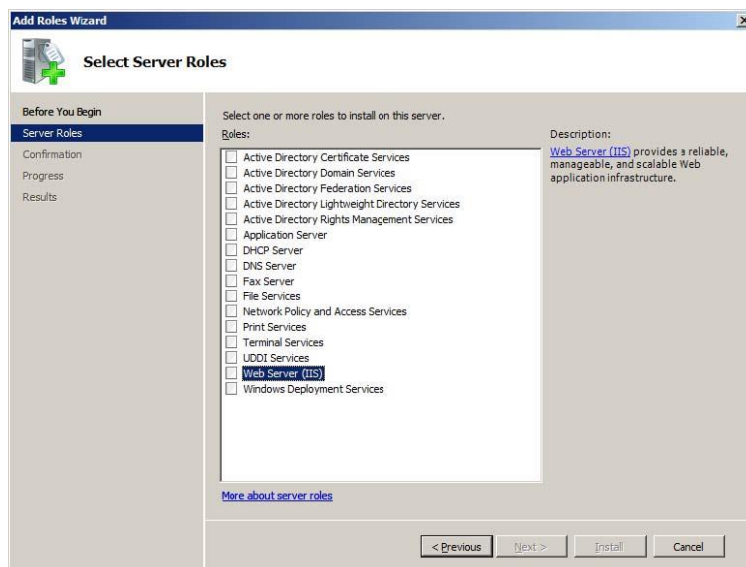
Important: Different software applications might require different IIS components to be installed. If additional IIS components are already installed, do not clear their check boxes because this might prevent other software from working correctly.

To install IIS for Windows Server 2008 or Server 2012

1. Click **Start**, point to **Administrative Tools** and then click **Server Manager**.
2. In the **Server Manager** window, under **Roles Summary**, click **Add Roles**.



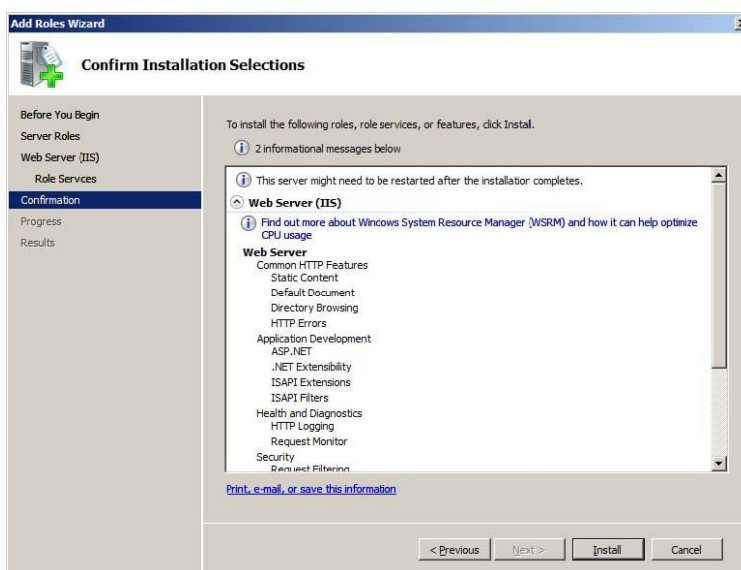
3. Use the **Add Roles Wizard** to add the **Web Server (IIS)** role.



4. To install the Web Server, some additional Windows features might need to be installed. In each case, click **Add Required Features**.



5. There is no need to make any selections in any of the dialog boxes that follow in the wizard. Accept the default selections at each step by clicking **Next** until all of the steps are complete.
6. At the end of the wizard, click **Install** to install the Web Server role and then follow the instructions on the screen.



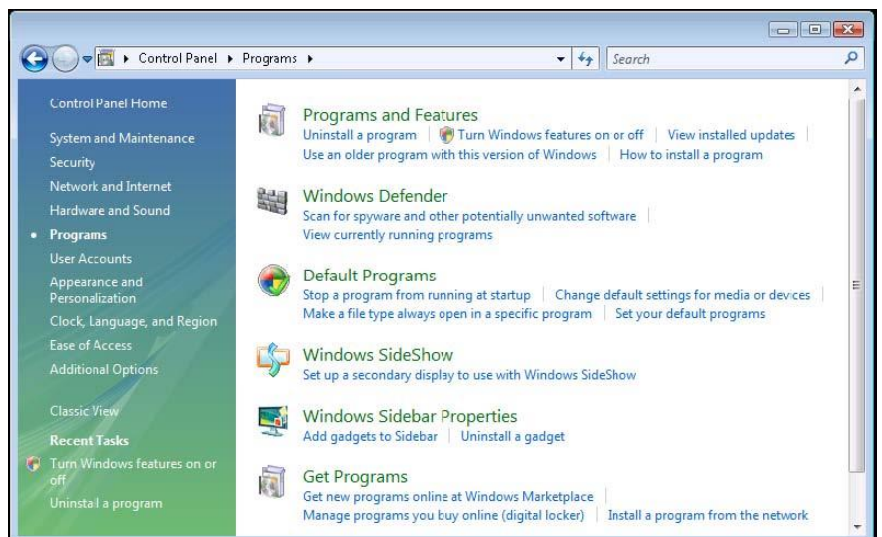
To install IIS for Windows 7, Windows 8, or Windows 8.1

1. Close all open Windows programs.

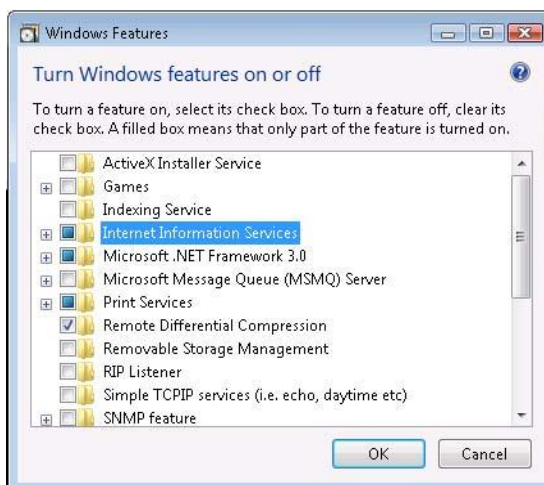
2. Open the Windows **Control Panel**, click **Control Panel Home**, and then click **Programs**.



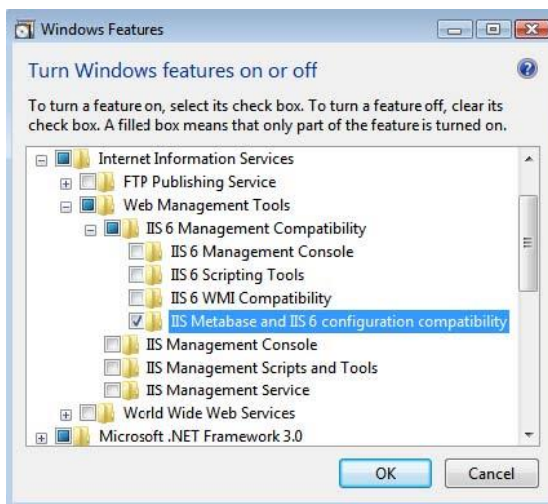
3. Under **Programs and Features**, click **Turn Windows features on or off**.



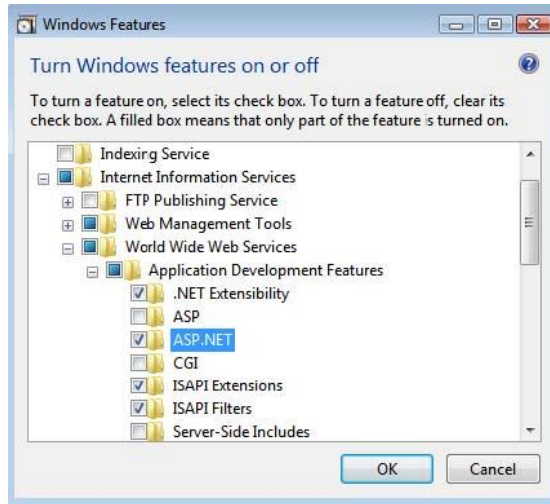
4. In the **Windows Features** dialog box, select the **Internet Information Services** check box.



5. Expand the **Internet Information Services > Web Management Tools > IIS 6 Management Compatibility** nodes and select the **IIS Metabase and IIS 6 configuration compatibility** check box.



6. Scroll down to expand the **World Wide Web Services > Application Development Features** nodes and select the **ASP.NET** check box. This feature automatically enables three other necessary features. Therefore, verify that the **.NET Extensibility**, **ISAPI Extensions**, and **ISAPI Filters** check boxes are also selected.



7. Scroll down to expand the **Common Http Features** node and then verify that the **Default Document** check box is selected.
8. Scroll down to expand the **Security** node and then verify that the **Request Filtering** check box is selected.
9. Click **OK**.

Install FactoryTalk Web Services

FactoryTalk Web Services can be installed from any FactoryTalk-enabled product CD that includes FactoryTalk Services Platform, version 2.10.02 (CPR 9 Service Release 2) or later. It is not installed automatically when you install FactoryTalk Services Platform.

For most applications, to use FactoryTalk Web Services with FactoryTalk-enabled products, we recommend that you install FactoryTalk Web Services on the computer acting as the FactoryTalk Network Directory Server. Your individual FactoryTalk-enabled products using FactoryTalk Web Services might also have specific installation requirements. For details, see the documentation supplied with your FactoryTalk-enabled product.

To install FactoryTalk Web Services:

1. Log on to Windows with a user account that is a member of the Windows Administrators group on the local computer.
2. Before installing FactoryTalk Web Services, install Microsoft Internet Information Services (IIS). See [Install Microsoft Internet Information Services](#) on [page 251](#).

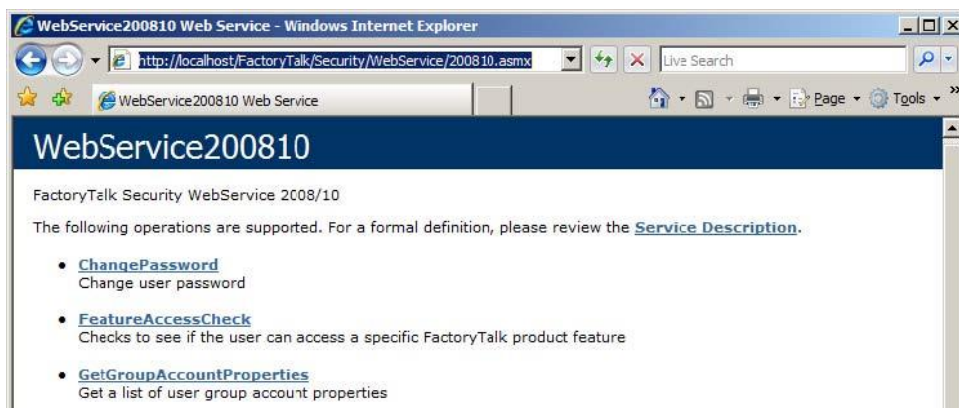
3. On the FactoryTalk Network Directory Server computer, click **Start > Control Panel > Programs and Features**.
4. In the list of installed programs, click **FactoryTalk Services Platform** and then click **Change**.
5. Follow the instructions on the screen to modify the existing installation.
6. In the list of program features, click **FactoryTalk Web Services** and then click **This feature, and all subfeatures, will be installed on local hard drive**.
7. Click **Next** and then follow the instructions to finish the installation.

To check that the FactoryTalk Security Web Service is working

If your computer is configured to use the **default port** for Web applications, or if you are not sure, open Internet Explorer on the computer where the FactoryTalk Security Web Service is installed and then navigate to <http://localhost/FactoryTalk/Security/WebService/200810.asmx>. To check that the FactoryTalk Security Web Service is working from a remote computer, paste the link into the Address box in Internet Explorer, and then substitute the name of the computer where the FactoryTalk Security Web Service is running for localhost.

When this link is opened for the first time, some operating systems might take several moments to respond.

If your computer is configured to use a **non-default port**, open Internet Explorer and then navigate to <http://localhost:81/FactoryTalk/Security/WebService/200810.asmx>, where **localhost:81** is the name of the computer and the port number, for example 81.

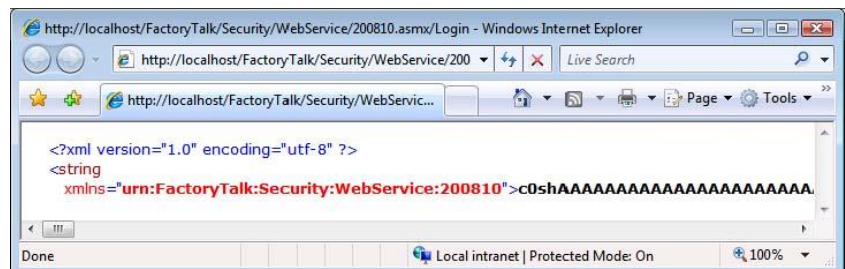


To check that you can log on to a user account using FactoryTalk Web Services:

If you have installed FactoryTalk Web Services on a network where a FactoryTalk Directory has already been configured with user accounts, you can test FactoryTalk Web Services to ensure that users can log on using the FactoryTalk Security Web Service.

You cannot run this test remotely; you must run it from the computer where the FactoryTalk Security Web Service is installed:

1. From the FactoryTalk Web Services page that appears when you click one of the two Web addresses mentioned in the "To check that the FactoryTalk Security Web Service is working" section above, click **Login**.
2. In the **userName** box, type the user name for an account already configured in the FactoryTalk Network Directory.
3. In the **password** box, type the password for the account.
4. In the **encryptionAlgorithm** list, type **ClearText** and then click the **Invoke** button. The FactoryTalk Security Web Service should return a login string.



If the logon fails and you are sure that you have typed the correct user name and password, the account might be disabled or locked. For details about enabling or unlocking the account, see FactoryTalk Help: On the Windows **Start** menu, click **All Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Help**. In the table of contents, click **FactoryTalk Security > User accounts > Reset a locked user account** or **Enable a user account**.

If the Web Service is not working

If FactoryTalk Web Services appear not to be working, check the following:

- Check your computer's network connection.

- Check that Internet Information Services is installed. See [Install Microsoft Internet Information Services](#) on [page 251](#).
- Check that .NET 3.5 SP1 is installed. .NET 3.5 SP1 is included on the FactoryTalk Services Platform CD, and is normally installed automatically with FactoryTalk Services Platform. You can see whether .NET 3.5 SP1 is installed by checking **Add or Remove Programs** or **Programs and Features** in the Windows **Control Panel**.
- If Internet Information Services is installed, IIS might be configured to use a port other than the default port 80. This might prevent FactoryTalk Web Services from communicating on that port. For details about changing the port, the default Web site uses, see the Microsoft knowledgebase article, [How to change the TCP port for IIS services](#) <http://support.microsoft.com/kb/149605>.

Tip: From the Windows **Command Prompt**, you can run `netstat -an |find /i "listening"` for a list of ports currently in use.

- Check your computer's firewall configuration.
 - If your computer is configured to use the **default port** for Web applications, or if you are not sure, open Internet Explorer on the computer where the FactoryTalk Security Web Service is installed and then navigate to `http://localhost/FactoryTalk/Security/WebService/200810.asmx`. To check that the FactoryTalk Security Web Service is working from a remote computer, paste the link into the Address box in Internet Explorer, and then substitute the name of the computer where the FactoryTalk Security Web Service is running for localhost.

When this link is opened for the first time, some operating systems might take several moments to respond.

- If your computer is configured to use a **non-default port**, open Internet Explorer and then navigate to `http://localhost:81/FactoryTalk/Security/WebService/200810.asmx`, where **localhost:81** is the name of the computer and the port number, for example 81.

If the FactoryTalk Web Services page appears, the firewall is configured correctly. If the page does not appear, configure the firewall manually. Either contact your company's Information Technology department for assistance, or to configure the firewall yourself, open the Windows **Command Prompt**, and then type

`"%systemroot%\System32\ netsh.exe firewall"`. Then use the **netsh.exe** command to add, delete, or modify the list of ports on which the firewall allows traffic. For details, see the Microsoft Knowledgebase article, [Netsh Command Syntax for the Netsh Firewall Context](#) <http://technet.microsoft.com/en-us/library/bb490617.aspx>.

What's a FactoryTalk Directory

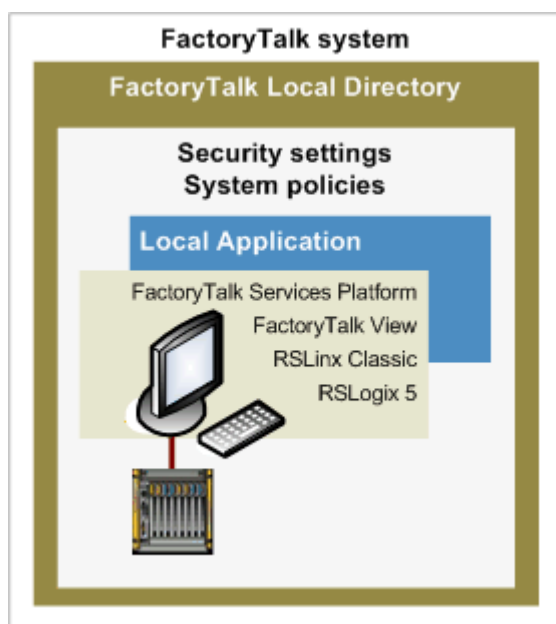
The FactoryTalk Directory references tags, data servers, security settings, and other project information from multiple data sources, and then makes this information available through a lookup service to all software products participating in that FactoryTalk system.

For example, tags are stored in their original environments, such as logic controllers, and graphic displays are stored in the HMI servers where they are created. Yet all of this information is available, without duplication, to any FactoryTalk product participating in the FactoryTalk Directory.

The FactoryTalk Directory can be either a Local Directory or a Network Directory. See [Understanding FactoryTalk Directories](#) on [page 262](#) for more information.

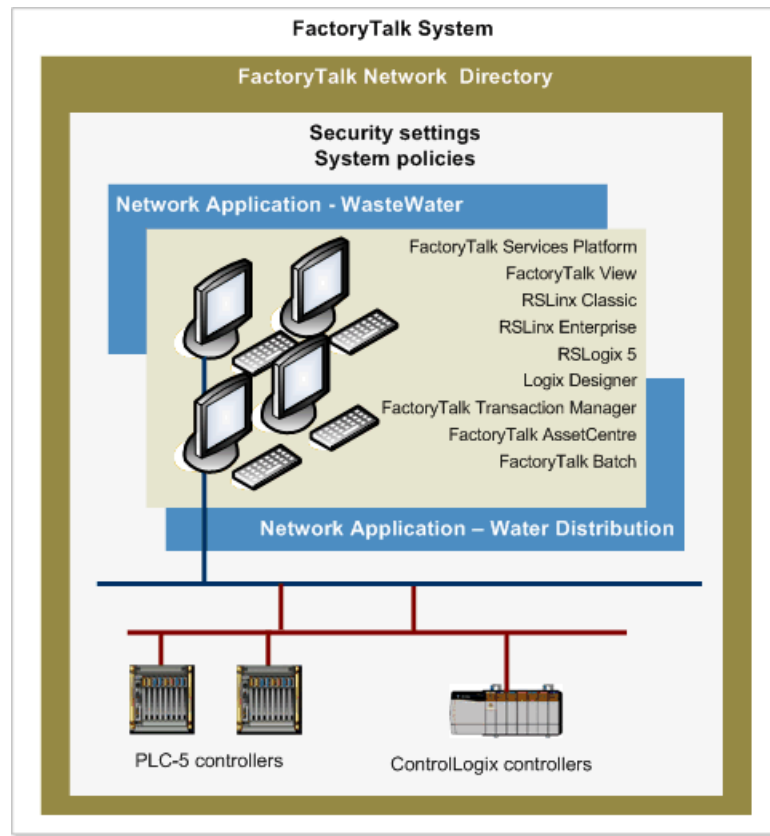
Creating your own FactoryTalk system

You can create a FactoryTalk system that suits the needs of your facility. For example, a FactoryTalk system may be as simple as FactoryTalk Services Platform, FactoryTalk View, RSLinx Classic, and RSLogix 5 all installed on the same computer, communicating with a single programmable logic controller, and all participating in the same Local Application held in a Local Directory.



Or a FactoryTalk system may be much more complex, with software products and hardware devices participating in multiple Network

Applications distributed across a network, all sharing the same Network Directory and FactoryTalk services.



Understanding FactoryTalk Directories

A single computer can host both a Local Directory and a Network Directory. The two directories are completely separate and do not share any information. If you use both directories, then that single computer participates in two separate FactoryTalk systems.

Both the Local Directory and the Network Directory support centralized security services, managed by FactoryTalk Security. Which directory you need depends upon which software products you plan to use and whether you plan to work in a stand-alone or networked environment.

Whether you are working with a Local Directory or a Network Directory, a FactoryTalk system is not necessarily constrained to a single application. Some of the FactoryTalk services and settings apply to all applications held in a directory, while others are specific to a particular application.

In the FactoryTalk Network Directory example above, the directory hosts two Network Applications: one named Waste Water and the other named Water Distribution. All of the areas, data servers, HMI servers, device servers, and alarm and event servers organized within each application are specific to that application. None of the application-specific information is shared with any other application in the directory. However, all of the information and settings organized within the System folder, such as security

settings, system policies, product policies, user accounts, and so on, apply to all applications held in the directory.

For example, if you created a new area in the WasteWater application and added a new Tag Alarm and Event Server, the change would not affect the Water Distribution application. However, if you changed a Security Policy, the change applies to both the WasteWater and Water Distribution applications. The setting would also apply to any other new applications created in the future in this same Network Directory.

Choosing a directory for FactoryTalk Security

The FactoryTalk Security services are integrated into both the FactoryTalk Local Directory and the FactoryTalk Network Directory. The table below shows which products require a Local Directory, which require a Network Directory, and which can use either directory.

Product	Network Directory	Local Directory
FactoryTalk Administration Console	Yes	Yes
FactoryTalk AssetCentre	Yes	No
FactoryTalk Batch	Yes	Yes
FactoryTalk Gateway	Yes	Yes
FactoryTalk Historian Classic	Yes	No
FactoryTalk Historian for Batch	Yes	No
FactoryTalk Metrics	Yes	No
FactoryTalk Portal	Yes	No
FactoryTalk ProductionCentre	Yes	No
FactoryTalk Scheduler	Yes	No
FactoryTalk Transaction Manager	Yes	No
FactoryTalk View ME	No	Yes ¹
FactoryTalk View SE	Yes	No
FactoryTalk View SE Local	No	Yes
Logix Designer	Yes	No
RSAutomation Desktop	Yes	No
RSBizWare BatchCampaign	Yes	Yes
RSBizWare eProcedure	Yes	Yes
RSLinx Classic	Yes	Yes
RSLinx Enterprise	Yes	Yes
RSLogix 5	Yes	Yes
RSLogix 500	Yes	Yes
RSLogix 5000	Yes	Yes ²
RSMACC	Yes	Yes
RSNetWorx	Yes	Yes
RSSECURITY Emulator	Yes	Yes

¹: The FactoryTalk Local Directory is not supported in FactoryTalk View ME 8.00 or later.

²: The FactoryTalk Local Directory is not supported in RSLogix 5000 software v20 and Logix Designer application v21 and later.

FactoryTalk Directory Configuration Wizard

The FactoryTalk Directory Configuration Wizard allows you to configure FactoryTalk Directory manually after you have installed FactoryTalk Services Platform. FactoryTalk Directory allows products to share a common address book, which finds and provides access to plant-floor resources, such as data tags and graphic displays.

Normally, all configuration of FactoryTalk Directory is done automatically during installation, and you do not have to run the FactoryTalk Directory Configuration Wizard.

When to run the FactoryTalk Directory Configuration Wizard

The FactoryTalk Directory Configuration Wizard is intended for use by FactoryTalk administrators.

Run the FactoryTalk Directory Configuration Wizard if:

- an error occurred while you were installing the FactoryTalk Services Platform, or a message appeared instructing you to run the wizard manually.
- you upgraded an existing FactoryTalk Directory from FactoryTalk Automation Platform version 2.0, but during the upgrade a valid FactoryTalk Administrator account could not be found for the directory.
- you renamed the computer after installing FactoryTalk Services Platform.
- you cannot access the FactoryTalk administrator account in the Network Directory or Local Directory. Running the wizard resets a locked administrator account, or allows you to change an expired password for the administrator account. Alternatively, have another user whose account is a member of the FactoryTalk Administrators group reset your locked account or password for you.

If your administrator account was disabled, have another user enable your account for you in FactoryTalk Administration Console. You cannot disable the last FactoryTalk administrator account in a directory. If no other user is available, or you do not know the password to another administrator account (for example, because that user left the organization), contact Rockwell Automation Technical Support.

Running the FactoryTalk Directory Configuration Wizard

On the computer where FactoryTalk Services Platform is installed, log on to Windows with a user account that is a member of the local Windows Administrators group. You must be logged on as a Windows administrator to run the FactoryTalk Directory Configuration Wizard.

1. On the **Start** menu, click **All Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Directory Configuration Wizard**.
2. Follow the prompts for configuring the Network or Local Directory.

For help with the options in any dialog box, click the **Help** button.

3

3.20 user account tab 196

A

about

- FactoryTalk systems 21
- this publication 11

accounts

- planning 70
- user 67

action groups 42, 49, 87

- assign permissions to 89
- creating 87
- creating new 90
- deleting 90
- editing 90
- renaming 91
- System folder 42
- working with 89

actions

- categories of permissions 83
- FactoryTalk Batch 50
- FactoryTalk Transaction Manager 50
- RSLinx Enterprise 50
- RSLogix 5 50
- RSLogix 500 50
- RSLogix 5000 50
- securing 49
- tag 54

activate

- FactoryTalk software 25
- RSLinx Enterprise 31

add

- logical name 108
- user accounts 184
- user accounts to FactoryTalk View ME 184
- user accounts to FactoryTalk View SE 162

additional resources 12

advanced features

- resource grouping 103

after restoring

- FactoryTalk Directory 236
- from an archive backup file 236

allow and deny permissions 80

application 21, 41

local 21

network 21

Application and Communications tabs 42

application authorization policies 95

application layer 18

Application tab 42

area 41

assign permissions 79, 83, 118

- best practice 80

- for RSLinx Classic 118

- to action groups 89

assign system policies 96

assumptions 223

audit policies 161

authenticated users 175

automation security 17

- overview 17

- understanding 17

B

back up

- best practice 177

- development application 192

- FactoryTalk Directory 231

- FactoryTalk Local Directory 192

- runtime application 192

Batch security 201

best practices

- assigning permissions 80

- back up local FactoryTalk Directory 177

- creating FactoryTalk user and groups 68

- creating group accounts 70

- denying permission 83, 141

- required rights 152

- using 3.20 user account tab 196

C

categories of permissions 83

- for actions 83

chain of inheritance

- breaking 81

client computer

- point to FactoryTalk Directory Server 46

- upgrading 242

common actions 51

- configure security 52
- create children 53
- delete 54
- execute 53
- list children 53
- read 51
- write 51
- Communications tab 42
- computer account 44
- computers and groups
 - System folder 44
- configure
 - Access Mode security 218
 - Equipment Editor security 217
 - FactoryTalk Batch product policies 209
 - feature security 99
 - multiple product features 99
 - multiple products 99
 - Recipe Editor security 217
 - RSLinx Classic 116
 - security 52
 - security for FactoryTalk Batch commands 213
 - security for FactoryTalk Batch View windows 210
 - security for RSLinx Classic 117
 - single product feature 100
- considerations when using RSLinx Classic with FactoryTalk 122
- controller resources
 - secure 141
- create
 - action groups 87
 - action groups for example scenario 87
 - Batch users and groups 204
 - children 53
 - exceptions for individual networks or devices 106
 - FactoryTalk Batch users and groups 204
 - FactoryTalk Security accounts 152, 177
 - new action groups 90
 - user accounts 67, 71
 - user group 74
 - your own FactoryTalk system 261

D

- default securable actions 49

- delete 54
 - action groups 90
 - unique identifier 76
 - user accounts 76
- development security 191
- development system
 - set up computers 223
- devices 44
- differences
 - securable actions vs. product policy feature security 49
- directory
 - choosing for FactoryTalk Security 263
- distributed system
 - example 24
 - upgrading computers in 242

E

- edit
 - action groups 90
- effective permissions 85
- e-mail addresses 71
- enable
 - FactoryTalk Batch View confirm settings 215
- enable security
 - for Logix Designer 126
- Equipment Editor
 - access modes 218
 - configuration options 219
 - security 217
- EvRSI activation 31
- execute 53
- Explorer window 40

F

- FactoryTalk
 - log on to 39
- FactoryTalk Activation 31
 - install 29
- FactoryTalk Activation Manager
 - install 29
- FactoryTalk Administration Console 39
- FactoryTalk Batch
 - actions 50
 - and FactoryTalk Security 201

- creating users and groups 204
- with FactoryTalk Security 201
- FactoryTalk Batch Server
 - create user account 33
- FactoryTalk Batch View
 - configure security for 209
 - configure View window security 213
- FactoryTalk Directory 21
 - after restoring 236
 - backing up 231
 - understanding 261
- FactoryTalk Directory Configuration Wizard 49
 - knowing when to run 265
 - running 266
- FactoryTalk Directory Server Location Utility 46
 - back up 192
- FactoryTalk Security
 - application layer protection 18
 - choose directory for 263
 - opening 38
 - overview 17
 - with FactoryTalk View ME 175
 - with FactoryTalk View SE 151
- FactoryTalk Security overview 17
- FactoryTalk Security Web Service
 - test 257
 - troubleshoot 258
- FactoryTalk Services Platform 21
 - installing 244
 - upgrading 241
- FactoryTalk system
 - about 21
 - creating 261
 - deploying 223
 - examples of 22
- FactoryTalk Transaction Manager
 - actions 50
- FactoryTalk user accounts 68
 - and Windows-linked user accounts 68
- FactoryTalk View ME
 - and FactoryTalk Security 175
 - configuring security for 177
- FactoryTalk View ME Station
 - Windows CE 175
- FactoryTalk View SE
 - and FactoryTalk Security 151
 - configuring security for 152
- FactoryTalk Web Services

- install 251
- installing 256
- test Security Web Service 257
- troubleshoot 258
- firewall
 - configure 258

G

- getting started 37
- give access
 - to secured controller resources 141
- graphic display
 - setting security on 184
- groups 44
- GUID 76, 196
 - deleting 76

H

- hardware required 12

I

- inheritance 81, 105
 - logical names 106
 - network relative paths 105
 - networks and devices 105
 - understanding 81
- install
 - FactoryTalk Activation 29
 - FactoryTalk Batch components 33
 - FactoryTalk Services Platform 28
 - FactoryTalk software 25
 - FactoryTalk View components 30
 - FactoryTalk Web Services 251
 - FactoryTalk-enabled software 27
 - Internet Information Services (IIS) 251
 - Microsoft Internet Information Server 251
 - Microsoft SQL Server 33
 - Microsoft SQL Server 2008 R2 Express 32
 - RSLink communications software 31
 - RSLogix software 32
 - RSSecurity Emulator 30, 114
- Internet Information Services (IIS)
 - Internet Information Services (IIS) 251

L

- list children 53
- Local and Network Directories 262
- local applications 21
- log on
 - FactoryTalk 39, 47
- Logix Designer
 - enable security for 126
 - secure controller resources 141

M

- manage multiple applications 191
- migrate ME Runtime 3.20 accounts 196
- multiple applications
 - FactoryTalk Security 191
- multiple system folders 183

N

- netsh command
 - configure Windows firewall 258
- netstat command
 - troubleshoot ports in use 258
- network applications 21
- Network Directory
 - specify location 45
- networks 44
- networks and devices 44
 - resource grouping 104
 - System folder 44

O

- order of precedence 82

P

- permissions
 - allow 80
 - assigning 79, 83
 - categories 83
 - deny 80
 - effective 85
 - explicit 81
 - inheriting 81
 - order of precedence 82
 - viewing 85

- plan your system 21
- planning to group resources 106
- PLCs and third-party OPC controllers
 - securing 147
- policies
 - application authorization 95
 - audit 161
 - product 43, 98
 - security 161
 - system 43, 161
 - System folder 43
 - user rights assignment 161
- ports
 - troubleshoot in use 258
- product policies 43, 93, 98, 160
 - and inheritance 98
 - inheritance 98
 - set up 160
- product policies and actions
 - how are they different 99

R

- read 51
- Recipe Editor
 - access modes 218
 - configuration options 219
- rename
 - action groups 91
- required
 - computer accounts 44
 - hardware 12
 - security permissions 231
 - software 12
- Resource Editor
 - using 107
- resource grouping 103, 104
 - Networks and Devices tree 104
- resource groups
 - planning 106
- resources
 - planning to group 106
- restore
 - application to the runtime computer 194
 - FactoryTalk Directory 233
- RSLinx
 - and FactoryTalk Security 113

RSLink Classic
 configure for FactoryTalk Security 116
 considerations 122
 networks and devices 44
 what can I secure 123
RSLink Enterprise
 actions 50
RSLogix
 actions 50
RSLogix 500
 actions 50
RSLogix 5000
 actions 50
 FactoryTalk Security 125
 with FactoryTalk Security 125
RSSecurity configuration
 importing 244
RSSecurity Emulator
 installing 114, 244
RSWho
 security settings 44
runtime security 191
runtime system
 set up computers 226

S

secure
 controller resources 141
 parts of a system 71
 PLCs and third-party OPC controllers 147
 user actions 49
security
 Batch View 209
 common actions 178
 settings 48
 tighten 55
security accounts
 creating 152
 creating in View ME 177
security authority identifier 231
security permissions
 inheritance 105
security policies 93
security policy
 require computer accounts for all computers 44
 User Rights Assignment 231

server 40
server computer
 upgrading 242
set security on a display 184
set up
 system and product policies 159
single sign-on
 logging on and off 61
 logging on as Administrator 63
 set up 61
 when to disable 64
software required 12
specify
 Network Directory location 45
stand-alone system
 example 23
system folder 42
 multiple 183
system policies 43, 93, 161
 assigning 96
 set up 161
system-wide policies 93, 95
 application authorization 95
 audit 93
 security 93
 user rights assignment 95

T

tag actions 54
 user action groups 55
 write value 54
test
 FactoryTalk Security Web Service 257
tighten security 55
 on a new system 55
 on an upgraded system 61
troubleshoot
 FactoryTalk Web Services 258
 ports in use 258

U

unique identifier 76
 deleting 76
upgrade
 client computers 242
 FactoryTalk Services Platform 241

- server computer 242
- user accounts
 - add to FactoryTalk View SE 162
 - adding to FactoryTalk View ME 184
 - creating 67
 - deleting 76
 - FactoryTalk 68
 - Windows-linked 68
- user action groups 55
- user group
 - create 74
- user rights assignment policies 93
- users and groups 45
 - System folder 45
- using
 - FactoryTalk Directory Configuration Wizard 265
 - Resource Editor 107
 - resource groupings 104

V

- viewing
 - permissions 85

W

- Windows Administrator account 47
- Windows CE
 - FactoryTalk View ME Station 175
- Windows firewall
 - configure 258
- Windows-linked user accounts 68
- working with
 - 3.20 user account tab 196
 - action groups 89
- write 51
- write value 54

X

- xvii 223
 - assumptions 223
 - on runtime system computers 226
 - setting up development system computers 223

Rockwell Automation support

Rockwell Automation provides technical information on the web to assist you in using its products. At <http://www.rockwellautomation.com/support> you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at <https://rockwellautomation.custhelp.com> for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit <http://www.rockwellautomation.com/services/online-phone> <http://www.rockwellautomation.com/services/online-phone>.

Installation assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator available at http://www.rockwellautomation.com/locations http://www.rockwellautomation.com/locations , or contact your local Rockwell Automation representative.

New product satisfaction return

Rockwell Automation tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the feedback form, publication [RA-DU002](http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf) http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Rockwell Automation Publication FTSEC-QS001K-EN-E

Supersedes Publication FTSEC-QS001J-EN-E

Copyright © 2015 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.